CAMERA DI COMMERCIO
DEL MOLISE

DISCIPLINARE PER I TRATTAMENTI RELATIVI ALLA VIDEOSORVEGLIANZA

ai sensi del Regolamento UE 2016/679, delle Linee guida n. 3/2019 dell'EDPB e delle indicazioni del Garante

1 - PREMESSA

1.1. – OBIETTIVI E CAMPO DI APPLICAZIONE

Premesse alcune indicazioni generali sulla disciplina della videosorveglianza, obiettivi del presente documento sono quelli di descrivere i principi, le regole e le procedure di:

A. gestione del servizio di videosorveglianza presso le aree di pertinenza della Camera di commercio del Molise (di seguito anche "Camera di commercio" o "Titolare" o "Ente"), ubicati all'ingresso delle sedi camerali di Campobasso ed Isernia considerati come siti soggetti a rischi;

B. trattamento, quali ad es., l'accesso alle immagini registrate e la realizzazione di copie di sicurezza, la loro conservazione e la consegna su richiesta, ad uso esclusivo delle Autorità (Magistratura e Forze dell'Ordine o altri soggetti, secondo le previsioni di legge)[1].

La procedura è di tipo organizzativo. Il suo fine è quello di:

1. individuare i soggetti autorizzati, evidenziandone ruoli, attività, compiti e responsabilità;
2. enunciare le direttive per una gestione delle immagini ed in particolare delle registrazioni in conformità con la legge vigente, tenuto conto delle esigenze concrete per cui il trattamento viene effettuato.

1.2. - RIFERIMENTI NORMATIVI PRINCIPALI

Il presente documento risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37, 38 e 39 del GDPR);
3. Responsabile esterno del trattamento dei dati (art. 28 del GDPR);
4. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
5. Artt. 32-36 del GDPR (sicurezza dei trattamenti e valutazione di impatto);
6. Attribuzione di funzioni e compiti a soggetti designati (art. 2-*quaterdecies* del D.Lgs. n. 196/2003);
7. EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (Versione 2.0), adottate il 29 gennaio 2020, in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it;

---

[1] Le "Forze dell'ordine" sono costituite dai corpi militari e civili dello Stato o degli enti pubblici territoriali, competenti alla tutela dell'ordine, della sicurezza pubblica e, se necessario, dei servizi di pubblico soccorso. L'art. 16 della legge n. 121/1981 comprende: la Polizia di Stato, l'Arma dei Carabinieri, la Guardia di finanza, nonché la Polizia penitenziaria e il Corpo forestale dello Stato (quest'ultimo, nel 2016, è stato sciolto ed il personale assegnato ad altre forze di polizia, in prevalenza nell'Arma dei carabinieri).

Fanno parte delle forze dell'ordine anche la Guardia costiera, che dipende dal Ministero delle Infrastrutture e dei Trasporti con ordinamento militare all'interno della Marina militare, nonché la polizia locale (detta anche "municipale"), di cui alla legge n. 65/1986 e successive leggi regionali specifiche.

Si tenga inoltre presente il concetto di "Autorità competente" previsto dal D. Lgs. 18 maggio 2018, n. 51 (*Attuazione della direttiva (UE) 2016/680 del parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*). L'art. 2, comma 1, lett. g), prevede che l'"autorità competente" è "1) qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; 2) qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica".

8. Garante per la protezione dei dati personali, Provv. 8 aprile 2010, in materia di Videosorveglianza;
9. Garante, *FAQ in tema di videosorveglianza*, in https://www.garanteprivacy.it/temi/videosorveglianza.

1.3. - ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE n. 679/2016 (General Data Protection Regulation)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali"
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo per la protezione dei dati - EDPB)
EDPB	European Data Protection Board v. WP29
RPD/DPO	Responsabile della Protezione dei Dati/ *Data Protection Officer*
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera di commercio di Molise
AdS	Amministratore di Sistema nominato sulla base del *DISCIPLINARE TECNICO PER LE FUNZIONI DI AMMINISTRATORE DI SISTEMA* della Camera di commercio del Molise, adottate ai sensi del GDPR e del Provv. del Garante del 27 novembre 2008 con Determinazione dirigenziale n. 65 del 16/05/2022

1.4. - MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione
(*cfr. stampigliatura di protocollo apposta in alto al presente allegato*)	Approvato	Prima emissione	Determinazione dirigenziale (*cfr. stampigliatura di protocollo apposta in alto al presente allegato*)

1.5. - ULTERIORI INDICAZIONI E RINVIO AD ALTRI DOCUMENTI

Il Disciplinare e le prescrizioni definite al suo interno, con specifico riferimento alle Parti da II a V (compresi i relativi allegati):

a) deve essere conosciuto e condiviso, ognuno per la propria Area/Servizio/Ufficio e per le mansioni di competenza. A questo riguardo sarà oggetto di una specifica attività di divulgazione/formazione;

b) devono intendersi quali istruzioni impartite dal Titolare, il cui mancato rispetto costituisce inosservanza delle disposizioni al personale;

c) integrano e completano, reciprocamente, le indicazioni contenute:

- nel "Disciplinare tecnico per l'utilizzo degli strumenti informatici, telematici e principali misure di sicurezza";
- nelle "Linee guida per la realizzazione di una valutazione di impatto del trattamento di dati (DPIA)".

2 - PARTE I – CENNI GENERALI SULLA DISCIPLINA DELLA VIDEOSORVEGLIANZA

2.1. – IL PROVVEDIMENTO DEL GARANTE E LE LINEE GUIDA DELL'EDPB

In via preliminare va fatto presente che, nel nostro ordinamento, non è presente una definizione che individui specificamente cosa si debba intendere per "videosorveglianza", né si rinviene una disciplina organica in materia. Il tema, infatti, è affrontato nell'ambito di norme specifiche, tra le quali – per i rispettivi ambiti – le disposizioni penali sul divieto di interferenze nella vita privata, la tutela del domicilio; le disposizioni del codice civile (e della legge sul diritto di autore), sulla tutela dell'immagine; lo statuto dei lavoratori, sul divieto di "monitoraggio", etc.

Il WP 29, nel parere n. 4/2004 (documento WP89), ha definito la videosorveglianza come l'"attività mirante al controllo a distanza di eventi, situazioni e avvenimenti" mediante l'"acquisizione di immagini, eventualmente in associazione con dati sonori e/o biometrici". Con riferimento ai 'componenti' di un sistema di videosorveglianza possiamo indicare i seguenti: a) mezzi di ripresa; b) mezzi di visualizzazione; c) mezzi di registrazione/archiviazione; d) mezzi di trasmissione/comunicazione. In tutti gli ambiti indicati trovano applicazione i principi del GDPR.

Il Garante, data la rilevanza dell'argomento[2], ha dettato una regolazione con il Provv. 29 aprile 2004, poi sostituito con il Provv. 8 aprile 2010[3]. Questo provvedimento – nella sua natura prescrittiva (essendo stato emanato ai sensi dell'art. 154, comma 1, lett., c), del Codice privacy)[4] – non è stato abrogato dal GDPR ed è ancora in vigore, ai sensi dell'art. 22, comma 4, del D.Lgs. n. 101/2018, secondo il quale "a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto".

Sulla videosorveglianza, il Comitato europeo per la protezione dei dati (EDPB – European Data Protection Board) ha predisposto delle «Linee guida sul trattamento dei dati personali attraverso dispositivi video», definitivamente adottate, nella versione 2.0., il 29 gennaio 2020.

Conseguentemente, i contenuti del citato Provvedimento del Garante devono essere letti tenuto conto delle intervenute disposizioni sia del GDPR che delle Linee guida dell'EDPB.

Nel prosieguo, anche in forma tabellare, saranno effettuati i confronti tra le indicazioni del Garante e quelle del Comitato (indicato anche come EDPB).

2.2. – AMBITO DI APPLICAZIONE DELLA DISCIPLINA

La disciplina sulla videosorveglianza, dal punto di vista del trattamento dei dati personali, trova applicazione nel caso di riprese di immagini di persone fisiche identificate o identificabili.

Le Linee guida dell'EDPB indicano tre esempi tipici di non applicazione:

---

[2] Secondo il Garante, «la raccolta, la registrazione, la conservazione e, in generale, l´utilizzo di immagini configura un trattamento di dati personali qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione)» nonché vi è la necessità di garantire, in particolare, un «livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, perché potenzialmente in grado di determinare un´ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati».

[3] Pubblicato nella G.U. n. 99 del 29 aprile 2010.

[4] Nel nuovo quadro di riferimento normativo, le Autorità di controllo non sono più dotate di poteri di regolazione generale.
L'art. 54 del GDPR prevede solo il potere di «indirizzo generale» attraverso linee guida, mentre il Codice privacy prevede: 1. l'emanazione di provvedimenti prescrittivi solo in circoscritte materie (trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati; trattamenti a fini di ricerca scientifica o statistici); 2. la sanzionabilità delle violazioni solo di alcune tipologie di provvedimenti (es., autorizzazioni generali, provvedimento che definisce le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute).

1) Il GDPR non è applicabile alle fotocamere false (vale a dire qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale). *Tuttavia, in alcuni Stati membri potrebbero essere applicabili altre normative.*

2) Le registrazioni ad alta quota rientrano nell'ambito di applicazione del GDPR solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.

3) Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica (ad esempio targhe o informazioni che potrebbero identificare i passanti), il GDPR non è applicabile.

Vengono ricordate anche due situazioni generali in cui non trovano applicazione le disposizioni del GDPR:

a) Trattamento di dati personali effettuato da una persona fisica nell'esercizio di una attività *esclusivamente* personale o domestica[5];
b) Trattamento di dati personali eseguito da parte delle autorità competenti per i fini di prevenzione, indagine, accertamento o perseguimento di reati, ovvero per l'esecuzione di sanzioni penali.

Riguardo la prima situazione, secondo quanto previsto dall'art. 2, par. 2, lett. c), del GDPR, esula dall'ambito di applicazione il trattamento per motivi personali (comprese anche le attività *on line*). Tuttavia, con riferimento alla videosorveglianza, detta deroga applicativa deve essere interpretata in modo restrittivo. Come stabilito dalla Corte di giustizia, la cosiddetta «deroga relativa alle attività a carattere domestico» deve *«[…] interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone»*[6].

Inoltre, un sistema di videosorveglianza, nella misura in cui comporta la registrazione e la conservazione costanti di dati personali e si estende *«anche se solo parzialmente, allo spazio pubblico, e pertanto è dirett[o] verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, [...] non può essere considerat[o] un'attività esclusivamente "personale o domestica" ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46»*[7].

Riguardo la seconda situazione, si rientra nel campo di applicazione della Direttiva 2018/680/UE, attuata in Italia con il D. Lgs. 18 maggio 2018, n. 51.

2.2.1. – Una ipotesi particolare: i finti sistemi di videosorveglianza

L'utilizzo di videocamere di sorveglianza non funzionanti (sin dall'origine) – nonostante non vi siano previsioni normative specifiche – determina alcune questioni a seconda che tale condotta sia tenuta da un soggetto pubblico, ovvero da un soggetto privato. Incide, inoltre, l'area che appare oggetto delle riprese. Ad una sommaria valutazione, dal momento che la videocamera è finta (e, come detto, non funzionante sin dall'inizio), non essendoci, pertanto, alcuna ripresa, ci si troverebbe di fronte ad un trattamento dei dati inesistente e, quindi, privo di qualsivoglia conseguenza.

Per completezza si tratteranno, in estrema sintesi, entrambe le situazioni.

Nell'ipotesi dell'installazione di un finto sistema di videosorveglianza da parte di un soggetto privato quello che incide sulla condotta è l'ambiente inquadrato dall'obiettivo. Se si tratta di un ambito interno alla sua proprietà esclusiva, il trattamento è inesistente. Inoltre, qualora il sistema fosse funzionante, non si

[5] In presenza di lavoratori all'interno dell'abitazione occorre però informarli della presenza delle telecamere per iscritto (informativa), precisando l'uso che si fa delle riprese.

[6] Corte giust. UE, sent. 6 novembre 2003, nella causa C-101/01*, Bodil Lindqvist,* punto 47.

[7] Corte giust. UE, sent. 11 dicembre 2014, nella causa C-212/13*, František Ryneš contro Úřad pro ochranu osobních údajů*, punto 33.

applicherebbe comunque il GDPR, ricorrendo la previsione indicata dall'art. 2, par. 2, lett. c)[8]. Sulla esclusione della disciplina della privacy ai trattamenti inesistenti il Garante si era già pronunciato con un provvedimento del 2003[9].

Qualora l'ambito inquadrato dalle finte telecamere non sia di diretta pertinenza del soggetto privato che le installa, si può incorrere nel reato di cui all'art. 615-bis cod. pen., concernente l'illecita interferenza nella vita privata, qualora ricorrano i presupposti applicativi[10].

Qualora l'installazione di finte videocamere sia effettuata da un soggetto pubblico, le conseguenze ravvisabili sono differenti.

Nell'ipotesi in cui queste "inquadrino" uno spazio pubblico o aperto al pubblico, si ingenera il legittimo affidamento delle persone che siano attivi strumenti di tutela e salvaguardia della propria integrità personale e patrimoniale. L'impossibilità di recuperare informazioni necessarie a tale tutela rende ovviamente impossibile disporre di elementi di prova da far valere in un giudizio penale o civile. Tale condotta può però determinare una responsabilità, a carico del soggetto pubblico, secondo la regola della responsabilità extracontrattuale, di cui all'art. 2043 cod. civ.

Particolare è il caso in cui l'installazione del finto sistema di videosorveglianza venga effettuata sul luogo di lavoro.

L'Installazione di sistemi di videosorveglianza sui luoghi di lavoro, secondo le regole dello Statuto dei lavoratori e le altre applicabili (si pensi ai contratti collettivi), prevede una specifica procedura che passa attraverso un previo accordo collettivo stipulato con associazioni sindacali, ovvero in alternativa previa

---

[8] Tranne, però, come detto, il caso in cui siano riprese persone (es: personale di servizio) che, oltre all'applicazione delle regole del diritto del lavoro, hanno il diritto al rispetto dei propri dati personali.

[9] "L´istallazione di una finta telecamera, non in grado di riprendere immagini o suoni, non comporta un trattamento di dati personali. Il ricorso presentato al Garante dalle persone che ritengono di essere state riprese, e relativo al trattamento delle informazioni eventualmente raccolte, è quindi inammissibile" (Garante, provv. 30 dicembre 2003, doc. web. n. 10846102).
Per le altre massime riferite alle decisioni del garante in materia di videosorveglianza si v. la rassegna pubblicata in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1048143.

[10] L'art. 615-bis cod. pen. Prevede, tra l'altro, la pena della reclusione da mesi 6 ad anni 4, nel caso in cui il reo si procuri notizie ed immagini della vita privata della vittima attraverso strumenti di registrazione e videoregistrazione che riprendano l'abitazione, la dimora, ed altri luoghi affini, del soggetto leso.
Per i presupposti applicativi v., per es., Cass. pen., Sez. III, 8 gennaio 2019, n. 372; Cass. pen., Sez. VI, 12 marzo 2020, n. 9932; Cass. 11 giugno 2015, n. 12139. In particolare, sull'installazione nei condomini di edifici, v. Cass. pen., Sez. V., 12 luglio 2017, n. 34151; Cass. pen., Sez. V, 21 ottobre 2008, n. 44156; App. Catania, Sez. II, 15 febbraio 2022.
Secondo una interpretazione, difficilmente accoglibile, l'art. 615-bis sarebbe applicabile, quale reato di pericolo (e non di danno stante la non applicazione analogica delle norme penali), in quanto la condotta punibile è ravvisata nella capacità di ingenerare, nella persona edotta della presenza della videocamera, *una situazione psicologica tale da modificare le proprie abitudini di vita*, a prescindere dall'effettivo concretizzarsi del danno, che risiederebbe nell'eventuale captazione e registrazione delle immagini che lo riguardano, evento impossibile in quanto la videocamera non è funzionante (ma la deterrenza si realizza proprio data la non conoscibilità di questa situazione da parte del soggetto ripreso).
Qualche possibilità di tutela penale può rivenirsi, invece, nell'art. 610 cod. pen., in materia di violenza privata. Nonostante l'opinione positiva delle corti di merito, secondo la Cassazione "L'uso di telecamere puntate sulla pubblica via non è di per sé illegittimo, se utilizzato per difendere beni primari, come la sicurezza o la proprietà privata, e purché le telecamere siano regolarmente segnalate". Nell'articolo invocato – continua la Corte - il requisito della violenza si identifica in qualsiasi atto o fatto, posto in essere dall'agente, che si risolva comunque nella coartazione della libertà fisica o psichica del soggetto passivo, il quale viene così indotto, contro la sua volontà, a fare, tollerare od omettere qualche cosa, indipendentemente dall'esercizio su di lui di un vero e proprio costringimento fisico. Tuttavia il delitto ex art. 610 c.p. "non è *configurabile, allorquando gli atti di violenza non siano diretti a costringere la vittima ad un "pati", ma siano essi stessi produttivi dell'effetto lesivo, senza alcuna fase intermedia di coartazione della libertà di determinazione della persona offesa"* (Cass. pen., sez. V, 13 maggio 2019, n. 20527).
In ogni caso, secondo la Suprema corte non è lecito collocare (in posizione non immediatamente visibile da estranei) in direzione della proprietà del vicino neppure una telecamera, anche finta (ad esempio un contenitore avente l'aspetto di una telecamera con un led ed una lampadina al suo interno) perché non può avere la finalità di scoraggiare eventuali malintenzionati ma l'esclusivo scopo di recare molestia allo stesso vicino: in tale ipotesi non vi è dubbio che ricorrano gli estremi dell'atto emulativo, di cui all'art. 833 cod. civ. (Cass. 11 marzo 2001, n. 5421).

autorizzazione rilasciata dall'Ispettorato territoriale competente[11]. Tale procedura riguarda, ovviamente, le telecamere funzionanti e non può essere applicabile quando queste ultime non siano funzionanti.

In ogni caso, secondo la giurisprudenza, la violazione della riservatezza dei lavoratori operata fuori dal regime di tutela delle norme in materia configura un illecito penale la cui natura è quella del reato di pericolo[12]. Risulta quindi irrilevante la capacità effettiva dell'apparecchio di registrare o meno, quello che interessa è la sua potenzialità lesiva nei confronti della psiche e del comportamento del dipendente.

Conseguentemente deve essere radicalmente esclusa la possibilità di installazione di finti sistemi di videosorveglianza, posta l'impraticabilità giuridica di accordi simulati in merito ai medesimi (cioè facendo credere che siano funzionanti, perché in tal caso la procedura di legge non può essere applicata).

2.3. – FINALITA' DELLA VIDEOSORVEGLIANZA

Provv. Garante	**Linee guida EDPB**
1) protezione e incolumità degli individui	1) protezione della vita e dell'integrità fisica delle persone
2) protezione della proprietà	2) protezione della proprietà e di altri beni
3) sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge	
4) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge	
5) acquisizione di prove	3) raccolta di elementi di prova in vista di procedimenti giudiziari civili
	Le finalità del monitoraggio devono essere documentate per iscritto (articolo 5, par. 2) e devono essere specificate per ogni telecamera di sorveglianza in uso (le telecamere utilizzate per lo stesso scopo da un unico titolare del trattamento possono essere oggetto di una documentazione unitaria)

[11] Di recente la Suprema Corte ha sottolineato che il necessario bilanciamento tra i diritti fondamentali della persona e il libero esercizio dell'attività imprenditoriale, comporta l'esclusione della configurabilità del reato "*quando l'impianto audiovisivo o di controllo a distanza, sebbene installato sul luogo di lavoro in difetto di accordo con le rappresentanze sindacali legittimate, o di autorizzazione dell'Ispettorato del Lavoro, sia strettamente funzionale alla tutela del patrimonio aziendale, sempre, però, che il suo utilizzo non implichi un significativo controllo sull'ordinario svolgimento dell'attività lavorativa dei dipendenti, o debba restare necessariamente "riservato" per consentire l'accertamento di gravi condotte illecite degli stessi*" (Cass. pen., sez. III, 27 gennaio 2021, n. 3255). Qualora il controllo abbia carattere diffuso sull'attività lavorativa, sarà sempre necessario installare il sistema di sorveglianza previo apposito accordo con i sindacati.

[12] Cass. pen., Sez. III, 30 gennaio 2014, n. 4331.

Si faccia attenzione che l'adozione della videosorveglianza – in specie negli ambienti di lavoro– non può avere quale finalità la prevenzione di possibili reati.

2.4. – BASE GIURIDICA

Affrontare il tema della base giuridica del trattamento dei dati, anche nella videosorveglianza, implica una riflessione sulle possibilità individuate nell'art. 6 del GDPR.

Provv. Garante	**Linee guida EDPB**
Il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici: • **trattamento consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2, del Codice previgente)** • nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice previgente)) • il trattamento di dati diversi da quelli sensibili e giudiziari è consentito… anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (art. 19, comma 1, del Codice previgente)	In linea di principio, ogni fondamento di diritto ai sensi dell'articolo 6, par. 1, può fornire una base giuridica per il trattamento dei dati della videosorveglianza. Ad esempio, **l'articolo 6, par. 1, lett. c), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto un sistema di videosorveglianza.** Tuttavia, nella pratica, le disposizioni più suscettibili di essere utilizzate sono: • art. 6, par. 1, lett. f): legittimo interesse • art. 6, par. 1, lett. e): **necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**

La base giuridica inerente "l'obbligo di legge" (art. 6, par 1., lett. c), del GDPR) deve essere interpretato in termini assolutamente restrittivi, nel senso che la disciplina legislativa (nazionale o europea) deve imporre l'adozione della videosorveglianza.

Conseguentemente, la tutela dei beni e del patrimonio, e/o delle persone (anche in relazione alla sicurezza delle medesime ex D. Lgs. 81/2008), non può costituire una valida base giuridica, ai sensi del citato art. 6, par. 1, lett. c), posto che, al momento, non vi è un «obbligo» di installare telecamere.

Nelle indicazioni contenute nel Provvedimento del Garante si indicano specifiche ipotesi nelle quali – come previsto da norme di legge – sono indicati precisi obblighi di legge, in correlazione con lo svolgimento di attività rientranti nelle finalità istituzionali degli enti pubblici.

Gli esempi del Garante, infatti, fanno riferimento solo a trattamenti «istituzionali» costituenti e "fondanti" la *mission* di un Ente pubblico, *quindi previsti da disposizioni legislative:*

- sicurezza urbana di competenza del Sindaco e dei Comuni (ordine e sicurezza pubblica, polizia giudiziaria, polizia locale, etc.)[13];
- deposito dei rifiuti, di competenza degli Enti locali (utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose; rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti ove sanzionabili);

[13] Cfr. l'art. 5, commi 2-*ter* e 2-*quater*, del D.L. 20 febbraio 207, n. 14, come convertito dalla L. 18 aprile 2017, n. 48; l'art. 6, commi 7 e 8, del D.L. 23 febbraio 2009, n. 11, come convertito dalla L. 23 aprile 2009, n. 38.

- rilevazione di violazioni al Codice della strada (anche qui: polizia locale e forze di polizia in generale);
- rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, di competenza del Sindaco e dei Comuni;
- controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (qui non serve una disposizione legislativa specifica, visto che si tratta di prestazioni sanitarie necessarie);
- sicurezza nel trasporto pubblico (sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi), anche qui di competenza degli Enti locali;
- tutela dei minori e degli anziani[14].

Secondo l'EDPB, al contrario, in presenza di una situazione di reale rischio, la tutela della proprietà da furti o atti vandalici può costituire un legittimo interesse con riguardo alla videosorveglianza.

Anche la base giuridica relativa all'esecuzione di **un compito svolto nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento** (art. 6, par. 1, lett. e) del GDPR), non è scevra di difficoltà, poiché occorre dimostrare che la videosorveglianza sia "necessaria" per la concretizzazione dell'interesse pubblico o per l'esercizio di pubblici poteri, situazioni – se del caso - già disciplinate, dal legislatore, ex art. 6, par. 1, lett. c), del GDPR.

In ogni caso, la base giuridica su cui si fonda il trattamento dei dati in questione deve essere stabilita dal diritto dell'Unione o dal diritto degli Stati membri ed è assolutamente necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Tale base giuridica, secondo quanto indicato dall'art. 2-*ter* del Codice – dopo le intervenute modifiche[15] – è quindi riconducibile:

a) ad una norma di legge;
b) ad un regolamento;
c) ad un atto amministrativo generale.

Nell'ambito del carattere di generalità ed astrattezza che caratterizza le prime due fonti del diritto, gli atti amministrativi generali non sembrano in grado di regolare fattispecie astratte, quanto, in via residuale, di fornire indicazioni su questioni specifiche nell'ambito di un quadro regolamentare già strutturato (da altre fonti).

Vediamo, di seguito, le altre possibili basi giuridiche indicate nell'art. 6, par. 1, del GDPR.

Altre basi giuridiche dell'art. 6, par. 1, del GDPR	Valutazione EDPB

[14] Per questa possibilità si v. l'art. 5-*septies* del D.L. 18 aprile 2019, n. 32, come convertito dalla L. 14 giugno 2019, n. 55. Per inciso né la norma né il decreto applicativo (D.M. 31 dicembre 2021) fanno alcun riferimento al trattamento dei dati personali.

[15] La modifica intervenuta con il D.L. n. 139/2021 (cosiddetto decreto "capienze"), convertito con modificazioni dalla Legge del 3 dicembre 2021, n. 205.

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Il consenso dell'interessato può fungere da base giuridica ai sensi dell'art. 7 GDPR solo in casi eccezionali[16]. Negli altri casi: • difficoltà nel dimostrare e documentare l'avvenuto previo consenso • problema della revoca Comunque, tale base giuridica non è mai invocabile in relazione ai dipendenti, dato lo «squilibrio di potere tra datori di lavoro e dipendenti»
d) salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	
f) perseguimento del legittimo interesse del titolare del trattamento o di terzi	**Il GDPR stabilisce chiaramente che le autorità pubbliche non possono invocare il legittimo interesse per i trattamenti svolti nell'esecuzione dei loro compiti** Sarebbe comunque necessaria una valutazione sulla consistenza del legittimo interesse, con documentazione ad es., di eventi lesivi su beni/persone ed una specifica valutazione - «bilanciamento di interessi» - sulla prevalenza dell'interesse vantato dal titolare rispetto ai diritti e le libertà fondamentali dell'interessato[17]

In assenza di una base giuridica derivante dall'obbligo di legge, ovvero dallo svolgimento dei compiti istituzionali, secondo quanto chiarito in precedenza, resta percorribile la strada del ricorso al "legittimo interesse", di cui all'art. 6, par. 1, lett. f), del GDPR.

Se è vero che il GDPR stabilisce che le autorità pubbliche non possono invocare il legittimo interesse è anche vero che questa preclusione concerne unicamente "i trattamenti svolti nell'esecuzione dei loro compiti", cioè per quelle che sono le loro funzioni istituzionali, sulla base del rispetto del principio di legalità.

Ciò significa che **il divieto di utilizzo dell'interesse legittimo non opererebbe nei confronti di una PA che agisce «*iure privatorum*»** (l'art. 1, comma 1 bis, della L. 241/1990, stabilisce che la PA nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato) ad es., in relazione alla protezione dei beni e del patrimonio. E' quindi difficile sostenere che, per la difesa del suo patrimonio, un Ente pubblico agisca in una veste totalmente diversa da quella di un qualsiasi privato.

Va notato che l'EDPB non fa alcun riferimento alle basi giuridiche di cui all'art. 9 (per i dati particolari) e 10 (per i dati relativi a condanne penali e reati) del GDPR, nonostante i «sistemi di videosorveglianza (…) possono rivelare dati di natura altamente personale e persino categorie particolari di dati», questi non sempre configurano un trattamento di dati particolari. Ciò perché il trattamento di questi dati personali richiede una specifica base giuridica *unicamente nelle ipotesi in cui il sistema di videosorveglianza sia stato predisposto effettivamente (e non solo incidentalmente) per la raccolta di tali dati particolari*.

Al riguardo, l'EDPB porta come esempi, i seguenti:

- ripresa di immagini di persone che partecipano ad una manifestazione politica o sindacale;

[16] Per esempio, il monitoraggio degli atleti per analizzarne tecniche e prestazioni.

[17] I Titolari del trattamento dovrebbero documentare gli eventi problematici in questione (data, modalità, perdita finanziaria) e le relative accuse penali, etc. Le situazioni di pericolo imminente possono configurare un legittimo interesse, ad es. nel caso di banche o negozi che vendono beni preziosi (ad esempio, gioiellerie) o di luoghi che sono notoriamente teatro di reati contro il patrimonio (ad esempio, stazioni di servizio).

- ripresa di immagini di pazienti in terapia intensiva.

Nelle due ipotesi, la base giuridica ravvisabile è, rispettivamente:

- l'art. 9, par. 2, lett. e), del GDPR (il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato) e
- l'art. 9, par. 2, lett. g), del GDPR (il trattamento è necessario per motivi di interesse pubblico rilevante).

2.5. – L'INFORMATIVA

Per la videosorveglianza – come per tutti i trattamenti – va osservato il principio di trasparenza, soprattutto perché le riprese costituiscono, con tutta evidenza, una "intromissione" nella vita personale degli interessati.

Sul tema, data la sua specificità, l'EDPB – nelle Linee guida in materia di trasparenza del 2018 – ha previsto due livelli, crescenti, di informativa.

L'informativa di "primo livello" è costituita da un "avvertimento", ossia in un segnale (anche grazie all'uso di una icona grafica), chiaramente visibile dall'interessato che serve a renderlo edotto del trattamento se varcato lo spazio soggetto alle riprese.

Detta informativa comprende, i dati essenziali per la tutela dell'interessato, nonché il "rinvio" su come e dove reperire l'informativa completa (che può anche essere compresa in un QR Code posto in questo primo livello di informativa).

L'informativa di "secondo livello" contiene, in dettaglio, quanto disposto dall'art. 13 del GDPR, con particolare attenzione a quelli che possono costituire espressione di maggiore presidio tutelare per l'interessato.

Ad esempio, appare utile indicare se vi sia (e chi è) un Responsabile del trattamento o se vi sono comunicazioni o trasferimenti all'estero di dati personali. Indicare anche la natura – pubblica o privata – del Titolare non è privo di valore.

Di seguito un quadro delle indicazioni del Garante e dell'EDPB che si completano vicendevolmente, con riferimento all'informativa di primo livello.

Provv. Garante	Linee guida EDPB

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. A tal fine, era proposto un modello semplificato di **informativa "minima"**, indicante il Titolare del trattamento e la finalità perseguita che:

- deve essere collocato **prima del raggio di azione della telecamera**, anche nelle sue immediate vicinanze [18];
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale;
- può inglobare un **simbolo** o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Il principio generale di trasparenza potrebbe estrinsecarsi in:

una «**informazione di primo livello**» (segnaletica di avvertimento) ad es., **un'icona accompagnata da un set di informazioni** (per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto) quali:

- le finalità del trattamento[19];
- l'identità del Titolare del trattamento;
- i recapiti del Responsabile della protezione dei dati;
- l'esistenza dei diritti dell'interessato.

Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato (ad es., trasmissione di dati a terzi, fuori UE…).

Occorre infine fare riferimento alle informazioni di secondo livello, più dettagliate, indicando dove e come trovarle.

Le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, **prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi**).

Di seguito, il parallelo delle indicazioni riferite all'informativa di secondo livello.

Provv. Garante	Linee guida EDPB

[18] In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno dovranno essere installati più cartelli.

[19] Gli interessati devono essere informati delle finalità del trattamento ai sensi dell'art. 13 GDPR. La semplice menzione di uno scopo di «sicurezza» o «per la vostra sicurezza» con riguardo alla videosorveglianza non è sufficientemente specifica (art. 5, par. 1, lett. b).

Il Garante riteneva auspicabile che l'informativa semplificata rinviasse a un **testo completo** contenente tutti gli elementi di cui all´art. 13, comma 1, del Codice previgente, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici, ad es. in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito

Le informazioni di secondo livello:

- devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del GDPR;
- devono essere facilmente accessibili per l'interessato, ad es., attraverso una pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso.

Dovrebbe essere possibile accedere al secondo livello di informazioni **senza entrare nell'area videosorvegliata**, ad es. tramite l'indicazione nell'informazione di primo livello:

- di un link o QR code
- di un numero telefonico da contattare

2.6. – ADEMPIMENTI GESTIONALI

2.6.1. – A) Autorizzazioni al trattamento

Sulle autorizzazioni al trattamento, il Garante ha sottolineato l'attenzione sui seguenti adempimenti:

a) designare per iscritto tutte le persone fisiche, *incaricate* del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti (distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni)[20];

b) osservare le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento.

L'EDPB, sul punto, nelle Linee guida non fornisce indicazioni. Ciò, probabilmente, perché si tratta di questioni "ordinarie" che attengono a qualsiasi trattamento di dati personali.

In questa direzione, le figure di riferimento, oltre – ovviamente – al Titolare, sono le seguenti:

- *Contitolare*. Nel caso di contitolarità è necessario indicare il soggetto con il quale è siglato uno specifico Accordo (ex art. 26 del GDPR), con particolare attenzione ai contenuti relativi alle attività svolte congiuntamente, ovvero individualmente e le relative ricadute, sia in termini organizzativi, che rispetto ai diritti degli interessati;
- *Responsabile esterno del trattamento*. La presenza di un responsabile, ex art. 28 del GDPR, per le attività di videosorveglianza, è una situazione abbastanza frequente, con l'obbligo – da parte del Titolare – di accertare (preventivamente ed in costanza di rapporto), la presenza ed il mantenimento dei requisiti richiesti per i trattamenti[21];
- *Soggetto autorizzato (o designato) al trattamento*. La designazione dei soggetti autorizzati (art. 26 del GDPR e art. 2-*quaterdecies* del Codice privacy) rientra tra le misure organizzative del Titolare e

[20] Ad. es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, etc.

[21] Le Linee guida dell'EDPB raccomandano al Titolare di inserire, nelle specifiche inerenti l'acquisto (o, comunque, la disponibilità) di un sistema di videosorveglianza, idonee clausole contrattuali inerenti il rispetto dei principi di *privacy by design* e di *privacy by default*, nel rispetto dei principi di cui all'art. 5 del GDPR. Il Titolare deve fare in modo di garantire – anche con la collaborazione del Responsabile – che la conformità al GDPR si applichi a tutti i componenti del sistema ed ai dati trattati, durante l'intero ciclo di vita del sistema e dei trattamenti.

richiede una specifica formazione, sia essa in termini generali sulla videosorveglianza, che con riferimento alle specifiche attività e procedure di trattamento svolte nell'ente;
- *Amministratore di Sistema*, Questo soggetto può essere esterno (ed allora valgono le indicazioni di cui all'art. 28 del GDPR), ovvero interno (ed allora è uno dei soggetti "autorizzati"). al quale si applicano le disposizioni in materia di Amministrazione dei Sistemi, con le specificazioni riguardanti anche la gestione del sistema di videosorveglianza.

La "preposizione" al trattamento (a parte il caso di contitolarità e di nomina del Responsabile esterno), segue l'attribuzione delle competenze 'funzionali' ascritte nella declinazione dell'assetto organizzativo dell'Ente che, per le funzioni "privacy", è anche noto con l'espressione "Organigramma privacy".

Infine, va ricordato il ruolo del RPD/DPO che, anche sulla videosorveglianza, assiste il Titolare (o Contitolare) nel rispetto delle disposizioni vigenti.

2.6.2. – B) Misure di sicurezza tecniche ed organizzative

Com'è noto il GDPR impone l'adozione, da parte del Titolare, di misure tecniche ed organizzative *adeguate* ai trattamenti che intende svolgere. La valutazione dell'adeguatezza è svolta preventivamente, ossia prima di effettuare il trattamento di dati personali.

Tra le principali disposizioni del GDPR si ricordano, al riguardo, le seguenti:

- il Titolare deve essere in grado di dimostrare la conformità del trattamento a quanto richiesto dal GDPR (art. 24);
- i dati personali devono essere protetti, in modo efficace, sin dalla progettazione del trattamento affinché, nello svolgimento del medesimo, siano già assicurati profili di tutela dell'interessato (art. 25, riguardo la *privacy by design*);
- i dati personali trattati devono essere solo quelli necessari per conseguire ogni specifica finalità di trattamento e l'impostazione predefinita del trattamento deve garantire la tutela degli interessati (art. 25 cit., riguardo la *privacy by default*);
- deve essere garantito un livello di sicurezza adeguato al rischio rispetto ai diritti e le libertà delle persone fisiche (art. 32).

Rispetto alle misure tecniche, le Linee guida dell'EDPB indicano quanto segue.

Le specifiche e la progettazione del sistema – ancor prima che venga messo in produzione - dovrebbero includere requisiti per il trattamento dei dati personali conformemente ai principi di cui all'art. 5, del GDPR.

Nel caso in cui un titolare preveda di acquistare un sistema di videosorveglianza commerciale, **deve includere questi requisiti nelle specifiche di acquisto**.

È necessario proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la **conservazione** (dati a riposo), la **trasmissione** (dati in transito) e il **trattamento** (dati in uso).

Vanno inoltre privilegiati sistemi che:

- consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati;
- non dispongano di funzioni non necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio);
- siano conformi a standard e specifiche tecniche per i sistemi multimediali (Ad es.: IEC TS 62045 – Sicurezza multimediale – Linee guida per la protezione della privacy di apparecchiature e sistemi in uso e fuori uso).

Provv. Garante	Linee guida EDPB
a) configurazione di diversi **livelli di visibilità e trattamento** delle immagini. Laddove tecnicamente possibile, i soggetti che accedono devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti, solo le operazioni di propria competenza	a) definizione e applicazione delle procedure per la **concessione, la modifica e la revoca dell'accesso** b) attuazione di metodi e mezzi di **autenticazione e autorizzazione** dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica
b) Implementazione di misure tecniche od organizzative per la **cancellazione integrale**, possibilmente in forma **automatica**, delle registrazioni, allo scadere del termine previsto	c) utilizzo di meccanismi di **cancellazione automatici**
c) Implementazione di sistemi di **protezione contro i rischi di accesso abusivo** (firewall/antivirus…)	d) utilizzo di soluzioni basate su hardware e software quali **firewall, antivirus o sistemi di rilevamento delle intrusioni** contro gli attacchi informatici
d) nel caso di trasmissione tramite rete pubblica (internet), applicazione di **tecniche crittografiche**; similmente per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).	e) **cifratura** dei dati f) protezione della trasmissione di filmati attraverso **canali di comunicazione sicuri** a prova di intercettazione;
	g) registrazione e revisione periodica delle azioni eseguite dagli utenti (**log**)
	h) esecuzione di **monitoraggio** e individuazione di **guasti** e risoluzione in tempi brevi delle carenze individuate (es., **ripristino dati**)

Quanto alle misure di sicurezza, sul versante organizzativo, la comparazione (e integrazione) tra le indicazioni del Garante e dell'EDPB, fornisce il quadro di seguito rappresentato.

Provv. Garante	Linee guida EDPB
	Oltre alla eventuale necessità di una **DPIA** (cfr. più avanti), il titolare del trattamento dovrebbe adottare un **piano di gestione appropriato**, stabilire e applicare **politiche** e **procedure** relative alla videosorveglianza.
a) limitare la possibilità, per i soggetti abilitati, di **visionare** non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare operazioni di cancellazione o duplicazione b) nel caso di **interventi di manutenzione**, limitare la possibilità di accesso alle immagini ai soggetti preposti (e solo se indispensabile per eventuali verifiche tecniche ed in presenza dei soggetti dotati	Il piano dovrebbe considerare i seguenti elementi: • definizione delle **responsabilità della gestione** e del funzionamento del sistema di videosorveglianza • finalità e ambito di applicazione del progetto di videosorveglianza • utilizzo appropriato e vietato (ad es.: dove e quando la videosorveglianza è consentita e dove e quando

di credenziali di autenticazione abilitanti alla visione delle immagini)	non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video) • misure relative alla **trasparenza** (informative) • modalità e **durata delle registrazioni video** • **formazione** specifica per gli autorizzati • specifiche istruzioni per la gestione: • degli **accessi interni** alle registrazioni video e per quali scopi • delle richieste di **accesso esterne** (esercizio diritti) • dei **problemi tecnici e procedure di recupero** • delle **violazioni di dati personali**

L'EDPB affronta anche il tema della sicurezza c.d. "fisica", al fine di proteggere le apparecchiature (e, quindi, i dati in esse contenuti) da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e da danni accidentali.

Tra le misure suggerite:

- tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video devono essere **protetti contro l'accesso fisico** non autorizzato;
- il **posizionamento dei monitor** (soprattutto quando si trovano in zone aperte, come una reception) deve consentire solo agli operatori autorizzati di poter visualizzare le immagini.

PRINCIPALI MISURE TECNICHE ED ORGANIZZATIVE IN MATERIA DI VIDEOSORVEGLIANZA SECONDO LE INDICAZIONI DELL'EDPB	
MISURE ORGANIZZATIVE	
Politiche e procedure	– individuare ruoli e responsabilità della gestione e del funzionamento del sistema di videosorveglianza; – stabilire e documentare le finalità e l'ambito di applicazione del sistema di videosorveglianza; – identificare gli impieghi consentiti e quelli vietati (ad esempio, uso di telecamere nascoste e registrazione audio oltre che video, riprese nei bagni, etc.); – adottare misure per garantire la trasparenza e gli obblighi di informazione; – definire le modalità e la durata delle registrazioni video, compresa la conservazione delle videoregistrazioni; – definire un piano della formazione specifica; – individuare le regole di autorizzazione all'accesso alle registrazioni e per quali finalità; – stabilire le procedure operative della videosorveglianza (ad esempio, da chi e da dove viene monitorata la videosorveglianza), – definire le procedure che devono seguire i soggetti esterni per richiedere le videoregistrazioni e le procedure per accogliere o respingere tali richieste;

	– definire le modalità operative a seguito dell'accoglimento delle richieste di accesso da parte di soggetti esterni; – stabilire le procedure per l'approvvigionamento, l'installazione e la manutenzione del sistema di videosorveglianza; – stabilire dal punto di vista organizzativo le procedure per la gestione degli incidenti e del data breach; – definire dal punto di vista organizzativo le procedure di continuità operativa e di data recovery.
MISURE TECNICHE	
Sicurezza del sistema e dei dati	– assicurare la protezione dell'intera infrastruttura della videosorveglianza (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti; – gestire la protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione; – adottare sistemi di crittografia delle immagini; – adottare soluzioni hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici; – adottare sistemi di monitoraggio su malfunzionamenti di hardware, software e interconnessioni; – adottare procedure tecniche per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di incidenti fisici o tecnici.
Controllo degli accessi	– adottare misure fisiche e logiche per consentire, ai soli soggetti legittimati, l'accesso ai locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in quelli in cui vengono conservate le riprese video; – definire le procedure per la concessione, la modifica e la revoca dei permessi di accesso fisico e logico; – curare che il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) consenta la visualizzazione ai soli operatori autorizzati; – verifica dei log e degli accessi fisici e soluzione delle carenze individuate.

2.7. – TEMPI DI CONSERVAZIONE

I dati personali oggetto di trattamento non devono essere conservati per un periodo superiore a quello necessario al conseguimento delle finalità del trattamento (art. 5, del GDPR). Questo principio vale anche per le immagini acquisite mediante sistemi di videosorveglianza.

L'EDPB ha stabilito che la tempistica della conservazione delle immagini dovrebbe essere valutata in termini **il più possibile ristretti**. In via generale, gli scopi legittimi della videosorveglianza sono spesso la protezione del patrimonio o la conservazione di elementi di prova ed è solitamente possibile individuare eventuali danni **entro uno o due giorni.**

Conseguentemente i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici.

Le indicazioni del Garante, quindi, su un periodo (massimo) di 7 giorni, non sono più cogenti.

Questo, tuttavia, non significa che non sia ammissibile la conservazione per un periodo superiore a 24-48 ore se siano accuratamente esplicitate le motivazioni inerenti lo scopo e la necessità di una conservazione per un periodo superiore.

2.8. – DIRITTI DEGLI INTERESSATI

L'EDPB ha fornito alcune indicazioni in relazione ai diritti degli interessati, con riferimento ad alcune fattispecie.

Diritto di accesso:

- non esercitabile per i trattamenti senza conservazione (monitoraggio in tempo reale);
- nel caso di richiesta di immagini in cui siano presenti anche terzi, si dovrebbero mettere in atto misure tecniche per soddisfare la richiesta di accesso, ad es. modifica delle immagini tramite mascheramento o cifratura;
- nel caso in cui il Titolare non sia in grado di identificare l'interessato che presenta richiesta, dovrebbe avviare una interlocuzione chiedendo che sia specificato nel modo più preciso possibile quando il soggetto è entrato nella zona di ripresa e/o ulteriori elementi utili all'evasione della richiesta;
- nel caso di cui al punto precedente, ove la richiesta non sia circostanziata e quindi possa essere ritenuta «eccessiva» (art. 12, del GDPR) il Titolare potrebbe addebitare un costo ragionevole all'interessato;
- se sono trascorsi i tempi di conservazione (e, quindi, le immagini sono state cancellate) l'interessato deve essere informato della circostanza.

Diritto alla cancellazione:

- conferma l'applicabilità delle eccezioni previste dall'art. 17 (tra cui: il trattamento è effettuato per un obbligo legale o interesse pubblico);
- la richiesta potrebbe essere assolta offuscando l'immagine dell'interessato, senza alcuna possibilità di recuperare successivamente i dati personali precedentemente contenuti[22].

Diritto di opposizione:

- vantabile in relazione a trattamenti posti in essere sulla base dell'interesse pubblico (e dell'interesse legittimo);
- prevede l'astensione del Titolare dal trattare i dati dell'interessato, salvo che non dimostri l'esistenza di motivi legittimi cogenti che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato deve vantare e addurre «motivi connessi alla sua situazione particolare» (ad es., particolari circostanze che potrebbero rivelare opinioni politiche o religiose, in grado di ledere i suoi interessi);
- in relazione alla videosorveglianza, l'accoglimento della richiesta potrebbe esplicitarsi nello spegnimento immediato della telecamera, per il tempo necessario a non riprendere l'interessato.

[22] Per rendere l'immagine non identificabile si adoperano, in genere, due tecniche: il c.d. "bleraggio" ed il c.d. "pixellaggio".
"Blerare" – che deriva dai verbi inglesi to *blear* (offuscare, sfocare) o *to blur* (annebbiare) – indica l'azione di 'offuscamento' delle immagini (si pensi ai volti dei minori o ai marchi d'impresa). Con il termine "Pixellare" (da pixel) s'intende, in un'immagine digitalizzata, "mascherare e rendere indistinguibile o irriconoscibile, mediante l'ingrandimento sproporzionato dei pixel, una scena, un particolare, o, molto spesso, il volto di una persona, specialmente se minorenne" (Dizionario Treccani).
Nonostante l'obiettivo identico le risultanze delle due tecniche possono dare risultati diversi a seconda, rispettivamente, del livello di offuscamento o di pixellaggio. Uno sfocamento estremo è generalmente irrecuperabile, il pixellaggio può invece essere "recuperato" mediante specifici software.

2.9. – VALUTAZIONE SULLA NECESSITA' DI EFFETTUARE UNA DPIA

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza potevano essere effettuati rispettando le misure e gli accorgimenti prescritti dall'Autorità ad esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (art. 17 del previgente Codice privacy).

La verifica preliminare era prevista quando vi fossero rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare. Ora detta verifica non è più prevista se non ad esito di una DPIA che attesti un rischio elevato per gli interessati (consultazione preventiva, ex art. 36 del GDPR).

Secondo l'art. 35 del GDPR, «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La valutazione d'impatto è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Il WP29 – ora EDPB – nelle *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*[23] ha identificano 9 criteri in presenza dei quali il trattamento potrebbe presentare un livello di "rischio inerente" potenzialmente elevato (in neretto si evidenziano i criteri applicabili, a seconda dei casi, alla videosorveglianza):

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione;
2. processo decisionale automatizzato che ha effetti giuridici o incida in modo analogo significativamente sui diritti degli interessati;
3. **monitoraggio sistematico;**
4. dati sensibili o dati aventi carattere altamente personale;
5. trattamento di dati su larga scala;
6. creazione di corrispondenze, combinazione o messa in relazione di due o più insiemi di dati;
7. **dati relativi a interessati vulnerabili;**
8. **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;**
9. impedimento agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Le Linee guida EDPB sulla videosorveglianza, oltre a richiamare il quadro normativo di cui sopra, specificano che, date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti

[23] WP 248 rev del 4 ottobre 2017.

sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d'impatto sulla protezione dei dati. I Titolari del trattamento dovrebbero quindi consultare l'elenco delle tipologie di trattamento soggette obbligatoriamente a valutazione d'impatto predisposte dalle Autorità nazionali, ai sensi dell'art. 35, par. 4, del GDPR.

Con il Provv. 11 ottobre 2018, n. 467, il Garante ha disposto l'«**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati**»

Le tipologie di trattamento indicate - redatte sulla base delle Linee guida WP 248 *ed allo scopo di specificarne ulteriormente il contenuto e a complemento delle stesse* - comprendono, tra gli altri:

- **monitoraggio sistematico**, utilizzato per osservare, monitorare o controllare gli interessati: questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
- **dati relativi a interessati vulnerabili:** il trattamento di questo tipo di dati è un criterio legato all'aumento dello squilibrio di potere tra gli interessati (dipendenti) e il Titolare del trattamento;
- **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative:** quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, etc.

Per l'effettuazione della DPIA, la Camere di commercio del Molise ha adottato una propria *"Procedura per la predisposizione di una valutazione di impatto sulla protezione dei dati personali (DPIA) ai sensi del Regolamento UE 2016/679"* (Allegato B alla deliberazione della Giunta camerale n. 58 del 15 luglio 2019).

Qualora il sistema di videosorveglianza sia già in esercizio, il Titolare deve verificare se sia necessario effettuare una DPIA. In ogni caso nella propria valutazione, potrà acquisire le informazioni eventualmente provenienti dalla valutazione d'impatto (o dalla documentazione tecnica) preparata dal fornitore del prodotto.

Si tratta di un aspetto importante perché la DPIA del fornitore (o analogo documento) potrà contenere dettagli in merito alla innovatività delle tecnologie utilizzate, alle misure di sicurezza presenti nel dispositivo tecnologico oggetto della valutazione del Titolare utilizzatore che, quindi, se opportunamente configurato, gli consentirà una adeguata gestione dei rischi e la dimostrazione del rispetto dei principi della *privacy by design* e *by default*, anche in assenza della formalizzazione di una apposita DPIA.

Si ricorda, al riguardo, che il Responsabile esterno del trattamento è tenuto a collaborare con il Titolare posto che l'art. 28, par. 3, lett. f), del GDPR, prevede che detto responsabile "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

2.10. – LE SANZIONI

Senza alcuna pretesa di completezza, anche sulla videosorveglianza si applicano le sanzioni:

a) amministrative pecuniarie, previste dagli artt. 82 e 83, del GDPR;
b) penali ed amministrative previste dal Codice privacy.

In particolare, le sanzioni riguarderanno, solitamente, le seguenti fattispecie:

- inosservanza dei principi generali di trattamento dei dati;
- carente o insufficiente adempimento degli obblighi di informazione;
- trattamento illecito per mancanza di una idonea base giuridica per il trattamento dei dati.

Considerato che il presente Disciplinare non riguarda la videosorveglianza dei lavoratori, si omettono le indicazioni sullo specifico regime sanzionatorio previsto dalla disciplina vigente.

In relazione alle sanzioni occorre interrogarsi sulla valenza delle indicazioni contenute nelle Linee guida dell'EDPB e se la loro violazione/inosservanza da parte del Titolare comporti l'applicazione di sanzioni.

In via di principio, i sopra citati artt. 82 e 83 non indicano tra le violazioni, le disposizioni adottate dall'EDPB. Tuttavia, l'art. 70 del GDPR stabilisce che le Linee guida del Comitato promuovono "l'applicazione coerente del presente Regolamento" hanno, cioè, natura interpretativa. Questa natura interpretativa riverbera i suoi effetti con riferimento, in particolare, all'obbligo del Titolare, ex art. 5, par. 1, lett. a), del GDPR, di trattare i dati personali dell'interessato "in modo lecito, corretto e trasparente". Il Comitato, con le sue valutazioni, concorre infatti all'applicazione "corretta" del GDPR, come indicato nell'art. 70, par. 1, lett. a).

Le conseguenze che si ravvisano sono, pertanto, le seguenti:

a) il rispetto da parte del Titolare delle indicazioni dell'EDPB fa presumere, fatte salve le valutazioni da parte dell'Autorità di controllo e di quella giudiziaria, la correttezza del trattamento;
b) il non rispetto delle indicazioni dell'EDPB, non costituisce prova della non correttezza, ma richiede una esplicita motivazione da parte del Titolare circa le modalità e le soluzioni adottate per i trattamenti svolti e la loro adeguatezza a quanto richiesto dal GDPR.

3 - PARTE II – ORGANIZZAZIONE

3.1. - MODELLO ORGANIZZATIVO PRIVACY

3.1.1. – Titolare e Contitolare

Il Titolare del trattamento è la Camera di commercio del Molise, con sede legale in Campobasso alla Piazza Vittoria n. 1 e sede secondaria in Isernia al Corso Risorgimento n. 302.

Secondo gli ordinari criteri di imputazione della volontà dell'Ente, il soggetto deputato, in relazione al presente trattamento, ad esprimere la volontà del Titolare è il Segretario generale, in quanto Delegato da quest'ultimo.

Per esercitare in concreto i suoi poteri, il Titolare si avvale delle figure individuate ai punti successivi.

3.1.2. – Delegato sostituto del Titolare

Il Sostituto per delega del Titolare è il Segretario Generale, in forza delle previsioni del Modello Organizzativo Privacy approvato con Deliberazione di Giunta camerale n. 58 del 15 luglio 2019.

3.1.3. – Designazione del Responsabile esterno del trattamento

Non sono stati designati Responsabili esterni del trattamento. La Società che ha proceduto all'installazione del sistema di videosorveglianza non dispone delle password di accesso per la visione delle immagini che sono a disposizione del solo Amministratore di Sistema: inoltre, in caso di malfunzionamento del sistema di videosorveglianza e a seguito dell'intervento effettuato, si procede automaticamente all'aggiornamento della password di accesso.

La Società che ha installato le telecamere non ha accesso al NAS dove risiedono le registrazioni.

Qualora la Camera dovesse far ricorso ad un Responsabile esterno, per la relativa nomina opererebbe in base a quanto indicato nelle apposite *Linee guida per i rapporti di contitolarità e per l'attribuzione di responsabilità a soggetti esterni* approvate dalla Camera di commercio del Molise con Determinazione dirigenziale n. 167/2022 e aggiornate con Determinazione dirigenziale n. 33/2023.

3.1.4. – Soggetti e personale autorizzato al trattamento

Autorizzato al trattamento è il dipendente soggetto all'autorità diretta del Titolare, da quest'ultimo autorizzato in ragione della funzione all'interno dell'Ente e più specificatamente l'Amministratore di Sistema.

Tenuto conto del quadro sopra delineato, a tali soggetti autorizzati sono affidati i seguenti compiti che si configurano anche come trattamenti:

a. accesso visivo al registrato, nei casi consentiti;
b. possibilità di realizzazione di copie di sicurezza, autorizzate dal Titolare;
c. presidio delle richieste di esercizio dei diritti dell'interessato, a norma degli artt. 15 ss., del GDPR, ferma restando la facoltà degli interessati di adire direttamente il DPO della Camera di commercio del Molise, i cui dati di contatto sono riportati nell'informativa fornita agli stessi;
d. informazione verbale e/o consegna dell'informativa dettagliata ex art. 13 del GDPR.

Il Responsabile Servizio di Prevenzione e Protezione della Camera di commercio del Molise, nominato ai sensi dell'articolo 17 D. Lgs. n. 81/2008, è coinvolto nell'ambito della gestione del servizio di videosorveglianza "esclusivamente lato sicurezza".

3.1.5. – Amministratore di Sistema

La Società che ha installato il sistema di videosorveglianza si avvale dell'Amministratore di Sistema dell'Ente designato con DS n. 9/2022, per la realizzazione delle seguenti attività:

a) configurazione e manutenzione degli impianti, compresa la creazione, la configurazione e la gestione tecnica dei profili utente;
b) configurazione del sistema automatico di conservazione massima dei dati (immagini) registrati.

4 - PARTE III – REGOLAMENTO DELLA VIDEOSORVEGLIANZA

4.1. – REGOLAMENTO PER LA VIDEOSORVEGLIANZA

4.1.1. – Principi fondamentali

Con il servizio di videosorveglianza con registrazione, il Titolare intende adottare una misura volta a migliorare la sicurezza delle aree (interne o esterne) di sua pertinenza, assicurando la protezione delle persone e del patrimonio dell'Ente, materiale ed informativo, tenuto conto della sensibilità del sito di rischio in ragione dell'alto valore delle risorse che vi sono concentrate.

L'attività di videosorveglianza non sostituisce né è complementare rispetto all'attività degli organi giudiziari o di polizia giudiziaria o delle forze armate o di polizia. L'utilizzo del sistema e delle registrazioni non deve prescindere dalle normative in vigore riguardanti i compiti degli Organi di Pubblica Sicurezza, di modo che la complementarietà del sistema si limiti a permettere l'attivazione delle Forze dell'Ordine, anche se col tramite del Titolare e dei suoi collaboratori.

Il trattamento dovrà pertanto avvenire nel rispetto dei seguenti principi:

1. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art. 5, lett. b), del GDPR).
2. I dati raccolti non possono essere utilizzati per finalità diverse o ulteriori e non possono essere diffusi o comunicati a terzi, salvo concrete esigenze di polizia o di giustizia.
3. Vanno rispettati i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili e stabilendo la localizzazione delle telecamere e le relative modalità di ripresa (art. 5, lett. c), del GDPR).
4. Gli interessati devono poter conoscere esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti, esercitando i diritti di cui agli artt. 15 ss. del GDPR.
5. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni di dettaglio, necessarie ai sensi dell'art. 13 del GDPR. L'informativa breve è affissa in prossimità delle aree oggetto di videosorveglianza e prima che l'interessato entri in dette aree.
6. L'informativa estesa è resa disponibile, secondo quanto indicato nell'informativa breve.
7. Occorre rispettare il divieto di controllo a distanza dei lavoratori e le garanzie previste al riguardo (art. 4, L. 300/1970, come modificato dal D. Lgs. n. 151/2015 (attuativo del c.d. *Jobs Act* L. n. 81/2015).
8. Occorre determinare il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, rispettando i tempi e le condizioni di legge. Gli interessati dovranno essere informati sui tempi di conservazione stabiliti dal Titolare anche al fine di poter esercitare i diritti loro attribuiti dal GDPR.
9. Occorre individuare, formare, autorizzare e istruire i soggetti che possono utilizzare gli impianti e prendere visione delle registrazioni, adottando procedure atte a garantire - secondo profili diversificati - l'accesso e la realizzazione di copie esclusivamente ai soggetti autorizzati. Tali soggetti sono in numero limitato, nominativamente identificati e dotati in via preventiva di specifici profili di autorizzazione, tali da consentire l'esecuzione delle sole operazioni necessarie e sufficienti all'assolvimento dei loro compiti. Sono soggetti all'autorità diretta del Titolare oppure del Responsabile esterno designato, secondo l'organizzazione di appartenenza e gli incarichi assegnati. Il personale è vincolato al segreto professionale.
10. I tecnici installatori e manutentori del sistema ed il personale tecnico informatico (in qualità di Amministratori di Sistema) potranno avere accesso ai sistemi per garantirne il corretto funzionamento. Essi possono avere accesso alle immagini solo se ciò è indispensabile, nei limiti ed in ragione delle operazioni che devono compiere. Il personale è vincolato al segreto professionale. Il Titolare, oppure il Responsabile esterno designato, secondo l'organizzazione di appartenenza e gli incarichi assegnati, dovranno redigere e tenere aggiornata la loro lista nominativa, anche in considerazione della loro

funzione di Amministratore di Sistema, ai sensi del Disciplinare tecnico per le funzioni di amministratore di sistema approvato con Determinazione dirigenziale n. 65 del 16/05/2022, in relazione al GDPR ed al Provv. del Garante 27 novembre 2008.

11. L'accesso visivo alle immagini, la loro registrazione e la loro trasmissione in rete deve essere protetta da misure di sicurezza idonee ad evitare ogni rischio di perdita, distruzione, accesso non autorizzato, trattamento illegittimo, non corretto o non conforme alle finalità dichiarate. In particolare, l'uso di apparati e sistemi digitali collegati in remoto, anche via wireless, devono implementare le misure di sicurezza richieste dalla normativa vigente, come specificate dal vigente Provvedimento del Garante e dalle Linee guida dell'EDPB.
12. Gli impianti dovranno essere configurati in modo da ridurre al minimo l'impatto sulla riservatezza degli interessati. Pertanto, non dovranno essere modificati gli angoli di ripresa o la definizione delle immagini, se non nel caso in cui ciò sia indispensabile a fronte di eventi anomali. Le funzionalità dei sistemi di controllo software devono essere configurate in modo che il loro impiego non risulti eccedente rispetto alla normale attività di videosorveglianza.

4.1.2. – Finalità del trattamento

La Camera di commercio del Molise effettua attività di videosorveglianza esclusivamente per garantire la sicurezza del patrimonio dell'Ente e delle persone che, a vario titolo, frequentano gli ambienti delle strutture o che accedono agli stessi.

In particolare, il controllo delle aree assicura:

A. l'individuazione e la gestione delle aree e dei punti strategici afferenti alla sicurezza;
B. il controllo di determinate aree che non possono essere presidiate con i normali mezzi, per garantire un elevato grado di sicurezza nelle zone monitorate;
C. la tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e terrorismo, improvvisi ed imprevedibili;
D. la tutelare della sicurezza delle persone che accedono alle sedi camerali per l'utilizzo delle sale di rappresentanza.

I dati trattati e raccolti mediante i sistemi di videosorveglianza con videoregistrazione, potranno essere utilizzati in sede di un eventuale giudizio civile o penale, per agevolare l'esercizio del diritto di difesa da parte del Titolare del trattamento.

4.1.2.1 – Esclusioni e divieti

A tutela dei lavoratori, **è vietato il trattamento delle immagini per qualunque finalità di controllo sull'attività dagli stessi svolte**[24].

Si esclude, inoltre, il trattamento per il perseguimento di finalità private e personali.
Fatto salvo l'esercizio dei diritti dell'interessato, a norma degli artt. 15 ss. del GDPR e l'ordine di una Autorità, le richieste di accesso alle immagini da parte di privati (compresi i lavoratori) per la tutela di un diritto non correlato alle finalità perseguite e dichiarate dal Titolare, devono essere mediate dall'ordine di una Autorità ed autorizzate dal Titolare. È fatto salvo il diritto degli avvocati, ai sensi dell'art. 391-*quater* del cod. proc. pen., ad avere copia delle immagini registrate (versando il costo eventualmente stabilito dalla Camera di commercio del Molise), a condizione che la richiesta motivata (anche tramite l'interessato) sia presentata in qualità di difensore di fiducia/d'ufficio dell'interessato indagato nell'ambito di un procedimento penale.

[24] La specificazione è necessaria poiché se il sistema di videosorveglianza riprende anche i lavoratori (es., in entrata/uscita), questo trattamento, che può risultare 'fisiologico', non può essere utilizzato in alcun modo ai fini del controllo sull'attività dei suddetti lavoratori, per il quale è necessario un diverso approccio disciplinare, secondo quanto previsto, in particolare, dall'art. 4 della legge n. 300/1970. Si veda, inoltre, l'art. 88 del GDPR e l'art. 111 del Codice privacy.

4.1.3. – Base giuridica

Le basi giuridiche dei trattamenti relativi all'utilizzo dei sistemi di videosorveglianza sono da ricondurre, ai sensi dell'art. 6, par. 1 del GDPR, alle seguenti lettere:

- *lett. e)* il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- *lett. f)* il trattamento è necessario per il perseguimento del **legittimo interesse** del Titolare del trattamento o di terzi.

La CCIAA potrebbe anche essere chiamata, nell'ambito di indagini vertenti su reati, a fornire copia delle immagini registrate dal sistema di videosorveglianza. In tal caso, il trattamento è operato sulla base degli **obblighi di legge** vertenti sul Titolare (art. 6, par. 1, lett. c, GDPR). Tali misure di tutela sono complementari e non sostitutive rispetto all'attività delle Forze dell'Ordine e dell'Autorità giudiziaria.
Per quanto attiene **il legittimo interesse del Titolare**, come indicato anche nelle Linee guida dell'EDPB, tale base giuridica è legittima se <u>necessaria per il perseguimento di uno scopo del Titolare</u> del trattamento che può derivare da un suo interesse legale, economico o non materiale.
È tuttavia necessario fare attenzione a che gli interessi del titolare non prevalgano sui diritti e le libertà fondamentali degli interessati, adottando le seguenti verifiche:

a) Verificare e dimostrare la sussistenza dell'interesse legittimo del Titolare;

b) Verificare e dimostrare che il trattamento dei dati personali è necessario al conseguimento dello scopo;

c) Verificare che le modalità del trattamento non determinino una situazione di squilibrio, a svantaggio dell'interessato, in relazione ai suoi diritti e libertà fondamentali.

Per quanto riguarda la lett. a), ad esempio, la tutela della proprietà e dei beni, può avere una diretta relazione con la tutela di beni di valore storico, artistico, etc., ovvero con la tutela delle persone fisiche siano essi i lavoratori che gli utenti dei servizi.

Rispetto alla lett. b), l'utilizzo della videosorveglianza va comparato con altre possibili soluzioni (esempio: un servizio di "ronda" con guardie private), evidenziandone anche l'incidenza in termini di costo per il Titolare.

Per quanto riguarda la lett. c), la videosorveglianza deve essere coerente con le esigenze del trattamento. Si pensi a telecamere di ampio raggio, con qualità di ripresa ad alta definizione, ovvero con la registrazione anche dell'audio, o, ancora, con meccanismi di riconoscimento biometrico, etc.

4.2 – MODALITÀ DI TRATTAMENTO

4.2.1. – Descrizione dell'impianto

Gli impianti e i sistemi di videosorveglianza installati presso i siti oggetto di protezione, consentono il trattamento di immagini riprese:

A. **con n. 1 telecamera esterna**, fissa senza zoom in alto sopra il portone d'ingresso collocata a presidio del perimetro e delle aree esterne del civico di **Campobasso Piazza della Vittoria n. 1**, collegata in rete wireless LAN su protocollo cifrato ad un registratore digitale sul posto. La registrazione è attiva in orario 0-24;
B. **con n. 2 telecamere esterne**, fisse senza zoom in alto a destra ed a sinistra sopra il portone posteriore collocata a presidio del perimetro e delle aree esterne dello stabile di **Isernia per l'ingresso su Via Liguria,** collegate in rete wireless LAN su protocollo cifrato ad un registratore digitale sul posto. La registrazione è attiva in orario 0-24;

C. **con n. 3 telecamere interne**, fisse collocate a presidio dei varchi portone principale, porta carraia e porta su scale interne di collegamento del piano terra dell'immobile condominiale di Via Scatolone e lo stabile al civico Campobasso Piazza della Vittoria, 1, collegate in rete wireless LAN su protocollo cifrato ad un registratore digitale sul posto. La registrazione è attiva in orario 0-24.
D. **con n. 2 telecamere interne,** fisse collocate a presidio dei varchi portone principale e pianerottolo porta posteriore dello stabile di Isernia relativamente all'ingresso principale con affaccio su Corso Risorgimento, collegate in rete wireless LAN su protocollo cifrato ad un registratore digitale sul posto. La registrazione è attiva in orario 0-24.

Tutti i registratori digitali sono ubicati in locali ad accesso ristretto e controllato, presso gli stabili di Campobasso, Piazza della Vittoria, 1, Piano sottotetto, Locale apparati di rete e Isernia, Corso Risorgimento 302, Piano primo, locale apparati di rete. Lo *storage* fisico dei registratori è protetto da crittografia.

Gli interventi tecnici, le modifiche e l'implementazione di nuove funzionalità dei sistemi di videosorveglianza, così come l'estensione delle aree oggetto di ripresa devono essere preventivamente autorizzati dal Titolare a seguito di valutazioni e parere positivo dell'Ufficio competente in materia Servizi Informatici della Camera di commercio.

Le apparecchiature presenti sono:
- N. 2 NVR 8 canali IP fino a 8 MP (recording), 2 canali a 8 MP/8 canali a 1080p (decoding), max. banda 160 Mbps, H.265+, 2 uscite video (1 VGA + 1 HDMI), 4 ingressi e 2 uscite allarme, 1 ingresso e 1 uscita audio bidirezionali, predisposto per montaggio di 2 dischi SATA (fino a 10 TB cad.), 1 porta RS232, 2 porte USB (2.0 e 3.0), 1 porta LAN 1000 Mbps + 16/8/4 porte PoE, 1U, alimentazione 100~240 Vac marca DAHUA modello NVR4208;
- N. 2 Dahua PFS3110-8T - Switch Layer 2 unmanaged con 10 porte Ethernet (8 10/100 mbps + 1 Gigabit + 1 Gigabit SFP), capacita switchin;
- N. 8 IR dome IP da esterno/interno IP67 antivandalo IK10, sensore CMOS progressivo 1/2.5", risoluzione 4K a 15fps, ICR, ottica zoom 5x motorizzata 7~35 mm ƒ1.4, luminosità 0.05 Lux ƒ1.4 (0 con LED On), portata LED IR fino a 100 m, 1 LAN 100 Mbps, 1 ingresso e 1 uscita di allarme, 1 ingresso e 1 uscita audio, IVS, privacy mask 4 aree, 3D, WDR (120 dB), face detection, micro SD card, alimentazione 12/24 Vdc/Vac/ePoE <15 W.

4.2.2. – Accesso logico

Le immagini sono accessibili in locale, tramite videoterminale collocato presso l'ufficio Servizi Informatici con visione in tempo reale e con possibilità di accesso al registrato presidiate dal personale addetto ai Servizi Informatici.

Per accedere alle immagini in tempo reale o registrate è necessario autenticarsi al sistema con specifiche credenziali di accesso (inserimento di username e password), previa attribuzione di un profilo utente personalizzato.

Il sistema non è impostato per tracciare e registrare gli accessi dell'Amministratore di Sistema, il quale ha la possibilità di connettersi anche da remoto per gestire eventuali malfunzionamenti.

4.2.3. – Collegamento da remoto alla centrale di controllo del Responsabile

Le immagini in tempo reale sono accessibili da remoto tramite applicazione sullo smartphone di proprietà dell'Amministratore di Sistema e previa autenticazione con specifiche credenziali di accesso (inserimento di username e password).

4.3. – DATA PROTECTION IMPACT ASSESSMENT (DPIA)

4.3.1. – Data Protection Impact Assessment (DPIA)

La DPIA in materia di videosorveglianza, alla quale si rinvia, è adottata dal Segretario Generale che provvede periodicamente alla verifica dei suoi contenuti e procede, ove necessario, alla sua revisione.

4.4. – AGGIORNAMENTO DEL REGISTRO DEI TRATTAMENTI

La procedura per l'attivazione (o la revisione) della videosorveglianza richiede che tutte le relative informazioni sui trattamenti vengano riportate all'interno del Registro dei trattamenti della Camera di commercio del Molise.

4.5. – INFORMATIVA

4.5.1. – Informativa agli interessati

Gli interessati devono sempre essere informati del fatto che stanno per accedere in una zona video sorvegliata tramite apposita informativa.

A tal fine, negli ambienti e negli spazi sottoposti a videosorveglianza, la Camera di commercio del Molise installa, in posizione chiaramente visibile, prima del raggio di azione della telecamera, appositi cartelli contenenti l'informativa semplificata conforme alle indicazioni stabilite dal Garante (simbolo della presenza di telecamere, identificativo del Titolare, finalità della raccolta, etc.). In allegato è riportato un modello-tipo di tale **informativa semplificata (v. Allegato 2).**

Nelle reception/accoglienza e nelle postazioni degli addetti alla sicurezza viene messa a disposizione degli interessati **l'informativa estesa**, contenente tutti gli elementi di cui all'art. 13 del GDPR, secondo il modello riportato **nell'Allegato 3.**

4.5.2. – Informativa ai lavoratori. Rinvio

Il presente Disciplinare – come detto – non riguarda la videosorveglianza dei lavoratori. Non si pone, pertanto, alcuna necessità di specifica informativa ai lavoratori medesimi.

4.6. – DURATA DEL TRATTAMENTO E TERMINI DI CONSERVAZIONE DELLE REGISTRAZIONI

Determinato un livello di rischio alto, in relazione alla sensibilità ed al rilevante interesse pubblico delle attività che vi si svolgono, nonché dei beni che vi si trovano, della valutazione storica e prognostica di possibili eventi illeciti e dannosi, alla ubicazione del sito di rischio, delle caratteristiche e dei limiti tecnici del sistema di videoregistrazione, il periodo di conservazione delle immagini si determina in 72 ore dalla loro rilevazione: tale tempo di conservazione è autorizzato dal Titolare al fine di garantire la conservazione delle immagini durante il periodo di chiusura settimanale dell'Ente (dalle ore 14.30 del venerdì alle ore 7,45 del lunedì).

Il limite del periodo di conservazione può essere superato solo per rispondere ad una specifica richiesta di custodire o consegnare una copia da parte dall'Autorità giudiziaria o dalle Forze dell'Ordine, in relazione ad un'attività investigativa in corso, ovvero negli altri casi previsti dalla legge (come per le indagini "difensive" dell'avvocato nei procedimenti penali). Qualora fosse necessario rispondere ad una richiesta dell'Interessato, si applica quanto previsto al successivo paragrafo 5.2., in tema di accesso alle immagini.

Qualora il risultato dell'analisi preliminare del rischio renda assolutamente necessaria una conservazione per un periodo superiore al termine massimo sopra indicato, prima di procedere alla impostazione del tempo di conservazione, si reputa necessario attivare la procedura di verifica presso il Garante.

4.7. – ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Mediante apposita istanza in forma scritta, indirizzata al Titolare nonché indirizzabile, in ogni caso, direttamente al DPO, anche consegnata tramite soggetti autorizzati al trattamento, l'interessato potrà esercitare i seguenti diritti:

a. ottenere conferma o smentita dell'esistenza di immagini che lo riguardano;
b. accedere ai dati che lo riguardano ed ottenerne copia;
c. verificare le finalità, le modalità e la logica del trattamento;
d. ottenerne il blocco, qualora i dati siano trattati in violazione di legge, nonché la cancellazione delle immagini registrate in difformità dagli scopi dichiarati nelle informative.

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione, in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

La risposta ad una richiesta di esercizio dei diritti riguarderà soltanto i dati attinenti al richiedente identificabile e le immagini che lo riguardano direttamente.

Di regola, l'accesso visivo alle riprese, alle registrazioni e la consegna di eventuali copie, se disponibili e tenuto conto dei tempi di conservazione delle stesse, è esclusivamente riservato alla magistratura ed alle Forze dell'ordine, nonché, come detto in precedenza, agli avvocati in caso di difesa dell'interessato in un procedimento penale.

Qualora risulti indispensabile concedere all'interessato il diritto di accedere visivamente alle immagini, se necessario dovranno essere adottate tecniche di schermatura (anche manuale) del video o programmi che rendano possibile l'oscuramento delle immagini che riprendono altri interessati.

La visione potrà comprendere eventuali dati riferiti a terzi soltanto se la scomposizione dei dati trattati o la privazione di alcuni elementi del video rendessero incomprensibili i dati personali dell'interessato.

Tutti gli accessi devono essere registrati mediante annotazione riportante data e ora dell'accesso, identificazione del richiedente, nonché gli estremi dell'autorizzazione all'accesso.

4.8. – REGOLE GENERALI DI COMPORTAMENTO DEGLI ADDETTI ALLA VIDEOSORVEGLIANZA

Di seguito sono indicate alcune regole generali di comportamento per gli addetti alla videosorveglianza:

a) L'addetto alla sorveglianza autorizzato a raccogliere, gestire e custodire le immagini, deve agire nei imiti delle istruzioni ricevute e secondo le procedure indicate nelle disposizioni di servizio.
b) Ove l'operatore incaricato ritenga che ciò non avvenga, non sia avvenuto o non possa avvenire, deve informane il proprio Responsabile del trattamento diretto (nella persona del superiore gerarchico o funzionale). Il Responsabile avviserà il Titolare del trattamento (o il Sostituto Delegato) al fine di adottare le misure ritenute opportune.
c) L'accesso alle immagini deve limitarsi alle attività oggetto della sorveglianza: devono essere ignorate eventuali altre informazioni di cui si possa venire a conoscenza, osservando il comportamento di un soggetto ripreso. In particolare, non dovranno essere date informazioni di alcun genere né attivate operazioni di ricerca, estrapolazione e copia delle immagini, richieste o sollecitate telefonicamente o verbalmente.
d) L'operatore incaricato non deve riferire a terzi estranei alcun elemento contenuto nelle immagini e nelle registrazioni o di cui comunque sia venuto a conoscenza nel corso della sua attività di sorveglianza. È altresì vietato duplicare le immagini (per es. fotografando lo schermo con il proprio smartphone personale) e quindi diffonderle, comunicarle o consentire l'accesso a soggetti diversi da quelli individuati nel presente Disciplinare, secondo la procedura per l'accesso alle immagini, di cui al successivo paragrafo 5.2.

e) L'operatore incaricato non ha autonomia decisionale e dovrà attenersi alle istruzioni ricevute. In caso di dubbio dovrà rivolgersi al proprio Responsabile del trattamento diretto e attendere istruzioni che devono essere fornite per iscritto.
f) L'operatore incaricato deve custodire con diligenza le immagini eventualmente in suo possesso, applicando le istruzioni e le disposizioni di servizio ricevute, nel rispetto delle regole previste dal presente Disciplinare.
g) L'obbligo di riservatezza non si applica ai rapporti con il Titolare né con il Responsabile esterno designato, con i superiori, con la magistratura e le Forze dell'ordine. In caso di dubbio, è fatto obbligo all'operatore incaricato di chiedere istruzioni scritte al Responsabile del trattamento di riferimento.

5 - PARTE IV – PROCEDURE DI GESTIONE

5.1. – GESTIONE DELLE IMMAGINI

5.1.1. – Trattamento delle riprese in tempo reale

Il trattamento deve essere effettuato in modo da **limitare l'angolo di visuale all'area effettivamente da proteggere**. Per quanto possibile, dovrà essere evitata la ripresa di luoghi circostanti e di dettagli che non risultino rilevanti (Principio della minimizzazione dei dati: art. 5, par. 1, lett. c), del GDPR).

La funzionalità di zoom dovrà essere utilizzata solo se indispensabile per verificare la effettiva sussistenza di un evento anomalo o se la ripresa ordinaria fosse resa inefficace dalle condizioni ambientali (luce, eventi atmosferici, presenza di ostacoli).

5.1.2. – Trattamento delle registrazioni

Devono svolgersi all'interno del complesso dell'Ente, in locali dove non vi sia afflusso di persone estranee alla Camera di commercio del Molise, le seguenti operazioni di trattamento:

1. registrazione delle immagini;
2. visione del registrato;
3. estrapolazione/scarico delle immagini dal sistema di registrazione;
4. realizzazione di eventuali copie di sicurezza;
5. consegna delle copie ai soggetti autorizzati.

Il trattamento è svolto dall'Amministratore di Sistema.

5.1.3. – Accesso ai locali da parte di soggetti diversi dagli incaricati

Eventuali **accessi fisici ai locali** dove si svolge il trattamento o dove sono collocati i registratori digitali da parte di persone diverse dall'Amministratore di Sistema, **devono essere autorizzati per iscritto, dal Titolare**.

L'autorizzazione deve riportare:

- identificativo dell'autorizzato;
- lo scopo dell'accesso (breve descrizione dell'attività autorizzata);
- se possibile: la durata dell'accesso (orario di entrata e di uscita dai locali) oppure la stima del tempo necessario per lo svolgimento dell'attività autorizzata.

L'autorizzazione viene comunicata agli incaricati del trattamento interni o esterni, i quali dovranno accertarsi dell'identità della persona autorizzata prima di consentirne l'accesso ai locali dove si svolge il trattamento.

5.1.4. – Modalità di conservazione dei dati registrati

Secondo il sistema, le immagini possono essere memorizzate:

1. all'interno del dispositivo di registrazione;
2. in supporti esterni ed asportabili.

Le copie di immagini (realizzate secondo la procedura di accesso prevista dal successivo paragrafo 5.4.), sono conservate solo per il tempo intercorrente tra la loro realizzazione e la consegna materiale al richiedente.

Il supporto deve essere etichettato (o contrassegnato) indicando:

- l'identificativo del richiedente (nome dell'Autorità o del pubblico ufficiale o dell'avvocato);
- la data della richiesta;
- la data e l'orario delle riprese originali.

Vanno evitati riferimenti che consentano di identificare direttamente gli interessati, o di collegarli esplicitamente ad eventuali illeciti, presunti o contestati.

I supporti etichettati devono essere riposti in un armadio (o simili, per es. cassaforte) dotato di serratura, accessibile solo da parte dell'Amministratore di Sistema. Il contenitore delle copie deve essere comunque ubicato in area ad accesso ristretto e controllato.

Le copie potranno essere consegnate soltanto all'Autorità o ai soggetti autorizzati che ne abbiano fatto richiesta. Le copie non ritirate devono essere distrutte secondo la procedura prevista dal successivo punto 5.1.6.

5.1.5. – Cancellazione dei dati registrati

Le immagini sono registrate con impianto digitale. Il sistema deve essere impostato in modo da cancellarle automaticamente e definitivamente secondo la tempistica stabilita e, comunque, entro i tempi di legge.

In caso di impossibilità di procedere automaticamente alla cancellazione, essa dovrà avvenire manualmente attraverso l'apposita funzionalità del registratore. Le operazioni dovranno essere effettuate nel locale dove è ubicato il registratore. Al loro termine l'Amministratore di Sistema dovrà verificarne il risultato.

5.1.6. – Distruzione dei supporti esterni

Eventuali supporti contenenti copie realizzate su richiesta degli aventi diritto e non ritirati entro i tempi stabiliti, dovranno essere fisicamente distrutti in modo da renderne impossibile la ricostruzione ed il recupero dei dati.

Memorie di massa quali chiavette o hard disk, in caso di riutilizzo controllato, dovranno essere preventivamente sottoposte a formattazione di basso livello mediante apposito software, in modo da rendere impossibile il recupero dei dati memorizzati in precedenza.

Qualora destinate alla consegna a soggetti diversi dagli incaricati allo specifico ambito di trattamento, non dovranno essere riutilizzate ma essere anche smagnetizzate e distrutte.

5.2. – ACCESSO ALLE IMMAGINI TRATTATE

5.2.1. – Tipologie di accesso e relative modalità

Si prevedono i seguenti tipi di accesso, secondo le regole generali e specifiche, che costituiscono la procedura per l'accesso descritta nel prosieguo.

Tipo di accesso	Contenuto	Documentazione
I) Acquisizione di copia delle registrazioni (ad uso esclusivo di Autorità o delle Forze dell'ordine, o avvocato nei casi previsti dalla legge)	Il richiedente è autorizzato o legittimato ad ottenere copia delle immagini registrate, riversate su di un supporto mobile. La ricerca delle immagini, la realizzazione delle copie e la loro consegna materiale avvengono a cura dell'Amministratore di Sistema	✓ Richiesta dell'Autorità o delle Forze dell'ordine; ✓ Autorizzazione / richiesta del Titolare ✓ Autorizzazione al ritiro dei supporti da parte di persona identificata (in caso di impedimento del rappresentante del Titolare o del Responsabile interno); ✓ Compilazione del Verbale di consegna.

II) Accesso visivo	Il soggetto legittimato o autorizzato accede alla sola visione delle registrazioni, previa loro ricerca da parte dell'Amministratore di Sistema	✓ Richiesta dell'Autorità o delle Forze dell'ordine; ✓ Autorizzazione / richiesta del Titolare; ✓ Esercizio dei diritti dell'interessato a norma degli artt. 15 ss. del GDPR.

5.2.2. – Accertamento dell'esistenza di immagini trattate

Prima di dar corso a qualsiasi richiesta, il Titolare (o il suo delegato) accerterà l'effettiva esistenza delle immagini, avvalendosi dell'Amministratore di Sistema.

All'esito – attraverso i competenti uffici – darà formale e immediata comunicazione al richiedente dell'esito positivo o negativo dell'accertamento.

In caso di accertamento negativo, dovrà precisarne i motivi (per es. l'interessato non risulta ripreso; le immagini sono state cancellate entro i tempi di legge indicati nell'informativa, etc.).

5.2.3. – Registrazione degli accessi

Tutti gli accessi - comprese le richieste a cui si è dato riscontro negativo - devono essere registrati mediante l'annotazione di **apposito Registro**, nel quale dovranno essere almeno riportati:

- Il tipo di accesso autorizzato (accesso visivo, rilascio di copie);
- la data e l'ora dell'accesso;
- l'identificazione del terzo autorizzato;
- gli estremi dell'autorizzazione all'accesso (data dell'autorizzazione e organo dell'Ente che ne ha concesso il rilascio).

Per il Registro degli accessi si rinvia, più avanti, al paragrafo 6.1.

5.3. – ACCESSO VISIVO

5.3.1. – Soggetti e personale abilitato all'accesso ai dati

L'accesso visivo alle immagini è consentito solo a:

Soggetto	Attività
Titolare del trattamento	Autorizza l'accesso. Tramite gli uffici competenti, presiede alla verifica ed alla tenuta (Compilazione e conservazione) del Registro degli Accessi.
Sostituto Delegato dal Titolare	Trasmette al Titolare le richieste di accesso. Se Delegato: autorizza l'accesso e vi presenzia, riferendo al Titolare; tramite gli uffici competenti, presiede alla verifica ed alla tenuta (Compilazione e conservazione) del Registro degli Accessi. Se Incaricato accede alle immagini in quanto necessario alle operazioni di trattamento.
Autorizzato al trattamento con specifico profilo di autorizzazione: Amministratore di Sistema	Trasmette al Titolare o al Responsabile esterno / Delegato del Titolare le richieste di accesso. Ricerca le immagini e presenzia agli accessi. Accede alle immagini in quanto necessario alle operazioni di trattamento.

5.3.2. – Terzi autorizzati all'accesso

Accedono visivamente alle immagini registrate:

Soggetto	Motivazione e legittimazione
Autorità Giudiziaria o le Forze dell'Ordine, o avvocato nei casi previsti dalla legge	Per indagini in corso, tutela di un diritto in giudizio, attività di prevenzione e repressione di illeciti. La richiesta si fonda su ordine, provvedimento o richiesta formale. Le Forze dell'ordine possono ottenere copia delle immagini, così come l'avvocato nei casi previsti dalla legge.
Interessato (soggetto ripreso)	Di regola, ne è escluso. Accesso eccezionale autorizzato formalmente da Titolare, in caso di: 1. comprovata e documentata necessità o di pericolo concreto e imminente; 2. esercizio dei propri diritti previsti dagli artt. 15 ss. del GDPR.

5.3.3. – Accesso da parte di una autorità o delle forze dell'ordine

L'accesso visivo alle immagini su richiesta o ordine di una Autorità o delle Forze dell'ordine, è disposto dal Titolare del trattamento o del suo Sostituto Delegato.

Al tal fine, l'Amministratore di Sistema che riceve la richiesta deve immediatamente darne notizia al Titolare. L'Autorità dovrà essere immediatamente avvisata sui tempi di conservazione.

Oltre all'Amministratore di Sistema incaricato di ricercare le immagini, all'accesso dovrà essere presente il Delegato del Titolare.

Se formalmente richiesto, potrà essere realizzata una copia delle immagini al fine di consentire l'accesso oltre detto termine.

Il Titolare, tenuto conto delle esigenze istruttorie e dei motivi dell'accesso, fisserà il giorno, l'ora ed il luogo in cui il richiedente potrà visionare le immagini e li comunicherà all'Amministratore di Sistema.

Qualora l'Autorità non richieda la consegna della copia delle immagini registrate, essa dovrà essere distrutta ad accesso ultimato.

5.3.4. – Accesso visivo da parte dell'interessato (soggetto ripreso)

Di regola, agli interessati (soggetti ripresi) non è consentito accedere, nemmeno visivamente alle registrazioni. Pertanto, l'accesso visivo deve considerarsi eccezionale e motivato da circostanze gravi, oggettive e supportate da idonea dimostrazione di tali circostanze.

L'interessato può chiedere al Titolare di essere autorizzato all'accesso visivo alle immagini ex art. 15 del GDPR. La richiesta dovrà essere presentata secondo quanto previsto dalla procedura di cui ai successivi punti 5.4.3. e 5.4.4., e dovrà indicare i motivi che rendono indispensabile l'accesso, allegandone adeguata documentazione se disponibile o necessaria in relazione ai motivi della richiesta.

La ricerca delle immagini è riservata all'Amministratore di Sistema, che applica la procedura di cui al successivo punto 5.4.5.

Nel caso di accertamento positivo, il Titolare (o il Sostituto Delegato) potrà disporre la conservazione temporanea di copia delle immagini e fisserà il giorno - non oltre 10 giorni dalla rilevazione - l'ora ed il luogo in cui il richiedente potrà visionare le immagini che lo riguardano direttamente, inviando all'interessato tempestiva comunicazione.

Le copie realizzate temporaneamente per consentire all'interessato l'accesso, a norma dell'art. 15, del GDPR, vanno conservate fino alla data di accesso visivo.

Una volta esercitato il diritto di accesso, in mancanza di una diversa disposizione da parte di una Autorità (per es. ordine di acquisizione), le immagini dovranno essere cancellate o i supporti distrutti.

5.3.5. – Conservazione dei dati registrati su richiesta dell'interessato (soggetto ripreso)

Qualora l'interessato, in veste di soggetto ripreso, ritenga di avvalersi di immagini per tutelare o esercitare un proprio diritto in giudizio, potrà richiedere la conservazione temporanea di eventuali registrazioni che lo riguardano. A tal fine, dovrà rivolgersi alle Autorità competenti, le quali ordineranno l'acquisizione delle registrazioni e/o la conservazione per un periodo superiore a quello di legge.

L'interessato dovrà presentare al Titolare, anche per il tramite del Responsabile designato, formale richiesta scritta e motivata. La richiesta dovrà essere presentata secondo quanto previsto dalla procedura di cui al successivo punto 5.4.3. e dovrà essere corredata da una copia di denuncia-querela, da cui risulti la richiesta di acquisizione delle immagini quali mezzi di prova.

Le operazioni di ricerca delle immagini sono riservate ai soggetti autorizzati al trattamento. All'interessato non devono essere rilasciate copie delle immagini registrate.

5.3.6. – Esercizio dei diritti da parte dell'interessato (soggetto ripreso) ex artt. 15-22 del GDPR

L'interessato, in quanto soggetto ripreso, può fare istanza:

1. al Titolare del trattamento, Camera di commercio del Molise;
2. al Responsabile della protezione dei dati (DPO) designato, indicato nella suddetta informativa.

L'eventuale esercizio dei diritti è condizionato dal preventivo accertamento dell'esistenza o meno di registrazioni che lo riguardano direttamente. A tal fine, il richiedente deve essere informato sui i tempi di conservazione delle immagini. Qualora la richiesta fosse soltanto verbale, il richiedente deve essere gentilmente invitato a compilare il modulo messo a disposizione dal Titolare.

Per facilitare il reperimento delle immagini di possibile interesse, l'istanza deve indicare:

- a quale impianto di videosorveglianza si fa riferimento;
- il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa;
- indicazioni sull'abbigliamento indossato, accessori ed altri elementi utili alla individuazione;
- presenza di altre persone;
- attività svolta durante le riprese.

Nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, deve essere data immediata comunicazione al richiedente degli elementi mancanti, in modo che egli possa integrare la richiesta.

Non possono essere accettate istanze presentate da persone diverse dal soggetto ripreso, fatti salvi i casi previsti dalla legge. A tal fine, il richiedente dovrà esibire un documento di identità in corso di validità i cui estremi dovranno essere registrati dall'incaricato, senza fare copia del documento stesso, da allegare alla richiesta. In caso di istanza pervenuta a mezzo posta (cartacea), si darà corso alla richiesta solo se corredata da copia di un documento di identità valido.

L'allegazione del documento non è necessaria se l'interessato abbia sottoscritto la richiesta con la firma digitale, ovvero sia stato riconosciuto con altri sistemi di identità digitale (CNS, SPID, CIE).

5.4. – REALIZZAZIONE E CONSEGNA DI COPIE

5.4.1. – Personale autorizzato

Possono accedere alle registrazioni ed alle copie, in quanto necessario alle operazioni di trattamento:

Soggetto	Attività
Titolare del trattamento	Autorizza la conservazione delle registrazioni ed il rilascio delle copie. Accede al contenuto delle copie in quanto necessario all'individuazione delle immagini richieste ed al controllo dello stato dei supporti.
Delegato Sostituto del Titolare	Trasmette al Titolare le richieste. Se delegato, autorizza la conservazione delle registrazioni ed il rilascio delle copie. Accede al contenuto delle copie in quanto necessario all'individuazione delle immagini richieste ed al controllo dello stato dei supporti. Custodisce i supporti e ne cura la consegna.
Autorizzato al trattamento con specifico profilo di autorizzazione, Amministratore di Sistema	Trasmette le richieste al Titolare o ai suoi delegati. Ricerca le immagini e ne realizza le copie. Accede al contenuto delle copie in quanto necessario all'individuazione delle immagini richieste ed al controllo dello stato dei supporti. Custodisce i supporti e ne cura la consegna.

5.4.2. – Soggetti terzi autorizzati ad ottenere copia delle registrazioni

L'accesso tramite acquisizione di copia delle registrazioni è riservato:

1. all'Autorità Giudiziaria o alle Forze dell'Ordine, dietro loro ordine (per es. provvedimento giudiziario, verbale, etc.) o previa loro formale richiesta, scritta e motivata. A tal fine, ricorrendone i presupposti di legge (per es. indagini in corso, tutela in giudizio di un diritto, attività di prevenzione del crimine o di un pericolo imminente, etc.) l'Autorità può ordinare un prolungamento dei tempi di conservazione delle immagini;
2. agli altri soggetti pubblici e privati, nei casi previsti dalla legge;
3. al Titolare e al Sostituto Delegato, previa formale richiesta scritta. Nel caso di un loro impedimento, i supporti contenenti le registrazioni potranno essere consegnate a persone di loro fiducia, preventivamente individuate e autorizzate per iscritto. I nominativi dovranno essere trasmessi agli operatori incaricati unitamente alla richiesta delle copie.

Non è prevista la realizzazione, né la consegna di copie a soggetti diversi da quelli individuati al punto precedente.

5.4.3. – Forma e contenuto della richiesta

L'Autorità richiedente (o il diverso soggetto, nei casi previsti dalla legge) deve presentare apposita istanza scritta al Titolare.

Al fine di verificarne la provenienza, l'istanza deve essere redatta, alternativamente, su:

- carta intestata dell'Autorità (o soggetto) richiedente;
- su modulo del richiedente, contenete gli estremi identificativi dell'Autorità;
- su modulo fornito dal Titolare.

In ogni caso, essa deve riportare la data di presentazione, la firma (o sigla) e gli estremi identificativi del pubblico ufficiale (o altro soggetto) richiedente.

Nel caso in cui il richiedente sia il Titolare o il Sostituto Delegato, dovrà essere consegnata all'operatore incaricato apposita richiesta scritta, da cui risulti quale operazione di accesso egli deve compiere:

1. ricerca delle immagini;
2. visione del registrato;
3. estrapolazione / scarico delle immagini dal sistema di registrazione;
4. realizzazione di eventuali copie di sicurezza;
5. consegna delle copie a soggetti identificati ed autorizzati.

Oltre agli elementi utili per facilitare il reperimento delle immagini di possibile interesse (per es. impianto di videosorveglianza di riferimento, data e ora in cui sono state effettuate le riprese di possibile interesse), l'istanza deve indicare le motivazioni per cui viene chiesta copia delle registrazioni (per es. indagini nell'ambito di un procedimento in corso avanti l'Autorità giudiziaria, etc.).

Nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data immediata comunicazione al richiedente, invitandolo alle necessarie integrazioni.

5.4.4. – Modalità di presentazione della richiesta

In caso di istanza su modulo dell'Autorità, essa deve essere presentata con modalità tali da garantire la certezza del mittente (PEC, Racc. A/R, etc.). Qualora sia presentata oralmente da un pubblico ufficiale, quest'ultimo deve essere adeguatamente informato e invitato a presentare richiesta scritta, avvalendosi eventualmente della modulistica a disposizione.

All'atto della presentazione dell'istanza, il richiedente deve essere informato circa i tempi di conservazione delle immagini. Nel caso in cui le immagini di possibile interesse non risultino conservate o siano state già cancellate ne dovrà essere data immediata comunicazione al richiedente.

Qualora l'istanza venga direttamente presentata all'Amministratore di Sistema, questi deve inoltrarla immediatamente al Titolare o al Sostituto Delegato.

A sua volta, il Sostituto Delegato procederà alternativamente:

- ad inoltrare la richiesta al Titolare, attendendo l'autorizzazione di quest'ultimo;
- se ne ha il potere e nei casi in cui è consentito (per es. assenza del Titolare, casi di necessità o urgenza), potrà disporre l'accertamento sulla effettiva esistenza delle immagini e la loro eventuale copia, riferendo al Titolare, nel più breve tempo possibile e, comunque, entro i termini previsti dalle istruzioni ricevute.

5.4.5. – Ricerca delle immagini e riproduzione in copia

Il Titolare – sulla base degli elementi contenuti nella richiesta - accerterà l'effettiva esistenza delle immagini, attivando tramite comunicazione scritta gli operatori incaricati con il necessario profilo di autorizzazione.

Gli operatori procederanno alla ricerca delle immagini, comunicandone l'esito al Titolare o al Sostituto Delegato (qualora egli non sia presente all'accesso).

Il Titolare o, in sua assenza, il Sostituto Delegato, dà comunicazione al richiedente (Autorità o Forze dell'Ordine, o altro soggetto legittimato nei casi previsti dalla legge) dell'esito positivo o negativo dell'accertamento.

In caso di:

a. accertamento negativo, dovranno essere precisati i motivi (per es. l'interessato non risulta ripreso; le immagini sono state cancellate entro i tempi di legge indicati nell'informativa, etc.);
b. accertamento positivo, dovranno essere comunicati al richiedente il giorno, l'ora ed il luogo in cui potranno essere prelevate le copie richieste.

Se durante la ricerca dovessero essere rilevate immagini:

- di fatti che integrano ipotesi di reato o altri eventi rilevanti ai fini dell'intervento delle forze dell'ordine;
- di qualsiasi altra situazione anomala afferente visitatori, dipendenti od al patrimonio.

L'Amministratore di Sistema informerà immediatamente il Titolare (o il Sostituto Delegato) attendendo istruzioni.

5.4.6. – Realizzazione e consegna di copie

Su formale richiesta del Titolare, gli operatori incaricati riverseranno sul supporto esterno le immagini da conservare. Il supporto dovrà essere etichettato e conservato, secondo quanto previsto al precedente punto 5.1.4.

I supporti contenenti immagini registrate non devono mai essere asportati dai locali dell'Ente in cui sono collocati. La consegna di eventuali copie richieste da una Autorità (o altro soggetto legittimato) avviene presso i locali individuati dal Titolare o dal suo Delegato.

Il Titolare, o il suo Delegato, stabilisce se la consegna materiale avverrà a mezzo di proprio personale autorizzato. In questo secondo caso, il Titolare o il suo Delegato, dovrà comunicare a quale dei propri dipendenti saranno consegnati i supporti, comunicandone il ruolo nell'Ente e il nominativo agli operatori. La persona autorizzata dovrà provare la propria identità esibendo un documento valido, da annotare nel registro accessi e nel verbale di consegna se già predisposto.

Al momento della consegna materiale al soggetto legittimato, dovrà essere redatto un apposito verbale, in cui dovranno essere indicati:

- riferimento alle immagini duplicate, come da etichettatura del supporto (per es. riprese in data XYZ, riferite a presunto illecito avvenuto in ABC);
- data e ora della consegna del supporto;
- tipo del supporto (CD, DVD, chiavetta USB, hard disk, etc.);
- identificativo e firma (o sigla) della persona o dell'ufficio che ha curato la consegna;
- identificativo e firma (o sigla) del ricevente (Ufficio del Titolare, pubblico ufficiale che ha curato il ritiro dei supporti.

Le copie realizzate su ordine dell'Autorità vanno conservate fino al momento del loro prelievo da parte del pubblico ufficiale incaricato dalla richiedente.

Qualora le immagini non fossero acquisite dall'Autorità entro il termine indicato dall'autorità stessa per il ritiro (o non fosse stata indicata alcuna scadenza), gli operatori incaricati ne daranno notizia al Titolare, che contatterà l'Autorità richiedente prima di disporne la eventuale cancellazione o distruzione dei supporti.

6 - PARTE V – REGISTRO ATTIVITA' DI VIDEOSORVEGLIANZA

6.1. – REGISTRO DELLE ATTIVITA' DI VIDEOSORVEGLIANZA

È istituito il Registro delle attività di videosorveglianza, costituito dai seguenti due Registri (o Sezioni):

a) Registro dei Soggetti autorizzati al trattamento per la Videosorveglianza;

b) Registro degli accessi e delle richieste di copie di dati della Videosorveglianza

I modelli per i relativi Registri sono riportati negli **Allegati 8 e 9.**

Il Registro delle attività di videosorveglianza è tenuto dall'Amministratore di Sistema della Camera di commercio del Molise che ne cura la compilazione, la verifica e l'archiviazione.

7 - PARTE VI – ELENCO DEGLI ALLEGATI

7.1. – ALLEGATI

Costituiscono Allegati al presente Disciplinare i seguenti:

Allegato 1 - Nomina del Responsabile esterno per la Videosorveglianza, ex art.28 del GDPR;

Allegato 2- Modello di cartello/informativa breve sulla Videosorveglianza;

Allegato 3 - Modello di Informativa estesa sulla Videosorveglianza, ex art. 13 del GDPR

Allegato 4 - Modulo per Accesso del Titolare o di un suo delegato ai dati della Videosorveglianza;

Allegato 5 - Modulo per l'accesso delle Autorità o delle Forze dell'ordine a dati/immagini della Videosorveglianza;

Allegato 6 - Modulo per l'esercizio dei diritti dell'interessato ai dati/immagini della Videosorveglianza;

Allegato 7 - Modello di verbale per la consegna di immagini da Videosorveglianza;

Allegato 8 – Classificazione dei soggetti autorizzati e Modello di Registro dei soggetti autorizzati al trattamento per la Videosorveglianza;

Allegato 9 - Modello di Registro degli accessi e delle richieste di copie di dati della Videosorveglianza.